SYNESIS
管理者マニュアル

Rev. 8.0.1.1

TOYO Corporation

目次

1. 本書について

本書は、SYNESIS の管理者向けマニュアルです。
モデルによって運用・管理に必要な各種設定や操作方法が異なりますので、ご利用前にお使いのモデルを確認してください。
SYNESIS のモデルについての詳細は「1.2.SYNESIS の種類」をご参照ください。
操作に不明な点が生じた場合には、ユーザガイドをご参照いただくか、弊社お問い合わせまでお問い合わせください。

1.1. 表記規則および略号

本書で使用する表記規則は、下記の通りです。

表記	**説明**
[メニュー / ボタン名]	操作画面上に表示されるメニュー名またはボタン名を意味します。
<キー名> <*variable*>	キーボード上のキーを意味します。 イタリックフォントの場合は、変数を意味します。この場合は、環境動作に合わせて適宜設定します。
「設定項目」	操作画面上の設定項目を意味します。
>	画面遷移を意味します。
`Command`	コマンド入力例を意味します。
[-option]	コマンド例で使用される場合、省略可能なオプションを表します。 “[]” で囲まれていないオプションは省略できません。
<argument>	コマンド表例で使用される場合、引数を表します。 (左記は引数 argument を表しています。)
{Arg1 | Arg2}	コマンド例で使用される場合、選択可能な項目を表します。 選択可能な項目は ”{}” に囲まれ、”|” で区切って並べられます。その中の一つを引数として入力してください。 （左記は選択可能な項目として Arg1 と Arg2 があることを表しています。）

なお、記号は特に断りがない限り、原則半角で表現します。

1.2. SYNESIS の種類

SYNESIS にはラックマウント可能な Distributed タイプと持ち運び可能なポータブルタイプがあります。
モデルによって作業手順が異なる部分もありますので、写真を参考にご使用の SYNESIS の種類を確認してください。

1.2.1. Distributed タイプ (1U)

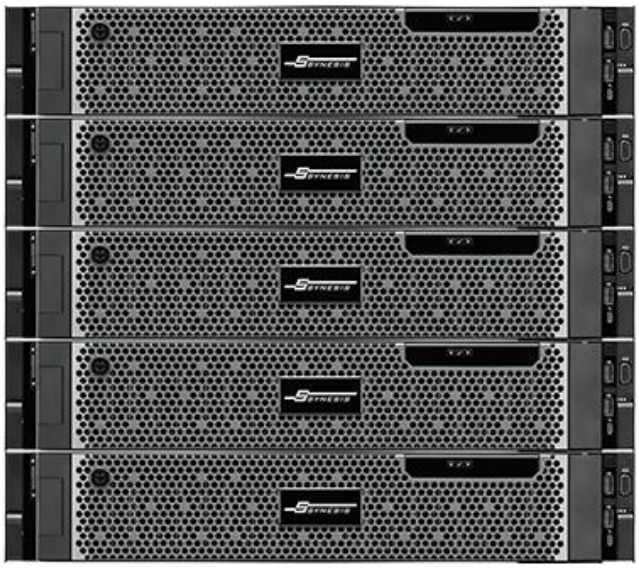
1 Uタイプのラックマウントです。

1.2.2. Distributed タイプ (2U)

2 Uタイプのラックマウントです。本体（コントローラユニット）のみになります。

1.2.3. Distributed タイプ (2U) ストレージユニット有

コントローラユニットと 1 台以上のストレージユニットのセットになります。



1.2.4. ポータブルタイプ

持ち運び可能なポータブルタイプです。

2. SYNESIS の起動・停止・再起動

本章では、SYNESIS の起動・停止・再起動手順について説明いたします。手順は、モデルによって異なりますので、ご利用のモデルに該当する手順を実施してください。

2.1. 起動

2.1.1. SYNESIS Distributed の場合

2.1.1.1. ストレージユニットの電源 On

1) ストレージユニット(MD1420/MD1400)がある場合は、背面の電源スイッチ 2 つを電源 On にします。
MD1420/MD1400 が複数ある場合、これらのどれから電源を On にしても構いません。

MD1420

MD1400

2) ストレージユニット(MD1420/MD1400)前面にある、HDD の緑色 LED の点滅が終わる(点灯状態になる)まで待ちます。

2.1.1.2. コントローラユニットの電源 On

ストレージユニットがある場合、それらの電源 On が完了していることを確認します。
コントローラユニット前面にある、電源ボタンを押します。

2.1.2. SYNESIS Portable の場合

SYNESIS ポータブルの電源ボタンを押し、電源を ON にします。

2.2. 停止

2.2.1. 共通手順

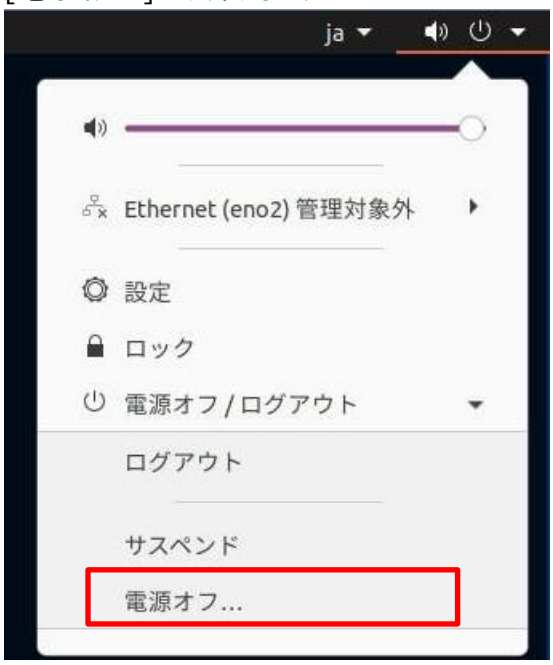
ご利用のモデルにかかわらず、以下の手順を実施します。その後ご利用のモデルに該当する手順を実施してください。

2.2.1.1. GUI(デスクトップ)から実施する場合

ローカルでキーボード、マウス、モニタを接続した状態で実施します。リモート実施は「2.2.1.2 SSH または Terminal から実施する場合」から実施してください。

1) デスクトップ画面右上のボタンをクリックし、[電源オフ/ログアウト] をクリックします。

2) [電源オフ...] をクリックします



3) ダイアログが表示されるので [電源オフ] をクリックします。

4) HDD の LED が消灯するまで待ちます。

5) ストレージユニットのある SYNESIS Distributed をご使用の場合、続いて「2.2.2.1 ストレージユニットの電源 Off」の記述に従ってください。

2.2.1.2. SSH または Terminal から実施する場合

1) PuTTY などのターミナルエミュレータを利用して、SYNESIS に SSH で接続します。
   接続先 :SYNESIS 管理ポートの IP アドレス
   ユーザ 名 (デフォルト) :synesis
   パスワード (デフォルト) :admin
2) 以下のコマンドを入力し、コントローラをシャットダウン(電源 Off)します。

```
$ sudo shutdown -h now
```

3) コントローラユニットの HDD の LED が消灯するまで待ちます。
4) ストレージユニットのある SYNESIS Distributed をご使用の場合、続いて「2.2.2.1 ストレージユニットの電源 Off」の記述に従ってください

2.2.2. SYNESIS Distributed の場合

2.2.2.1. ストレージユニットの電源 Off

1) ストレージユニット(MD1420/MD1400)がある場合は、「2.2.1.1 GUI(デスクトップ)から実施する場合」または「2.2.1.2 SSH または Terminal から実施する場合」が完了していることを確認し、MD1420/1400 背面の電源スイッチを Off にします。MD1420/MD1200 が複数ある場合、これらのどれから電源を Off にしても構いません。

MD1420

MD1400

2.3. OS の再起動

2.3.1. GUI (デスクトップ)から実施する場合

1) デスクトップ画面右上のボタンをクリックし、[電源オフ/ログアウト] をクリックします。

2) [電源オフ...] をクリックします

3) ダイアログが表示されるので [**再起動**] をクリックします。

2.3.2. SSH または Terminal から実施する場合

1) PuTTY などのターミナルエミュレータを利用して、SYNESIS に SSH で接続します。

接続先 :SYNESIS 管理ポートの IP アドレス
ユーザ 名 (デフォルト) :synesis
パスワード (デフォルト) :admin

Terminal で実施する場合は、SYNESIS の OS 上で Terminal を起動します。

2) 以下のコマンドを入力し、OS を再起動します。

```
$ sudo reboot
```

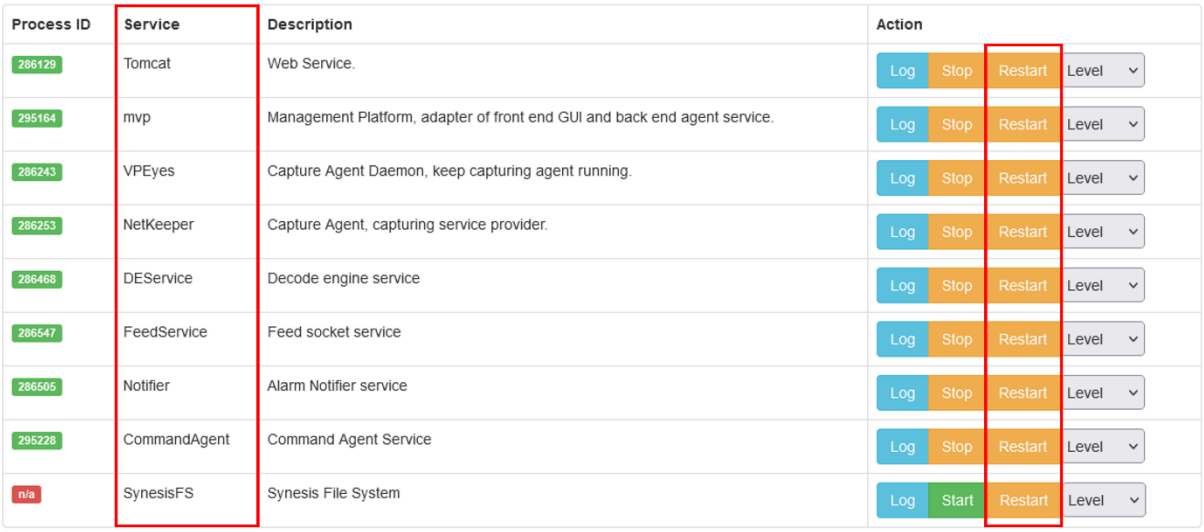
または、

```
$ sudo shutdown -r now
```

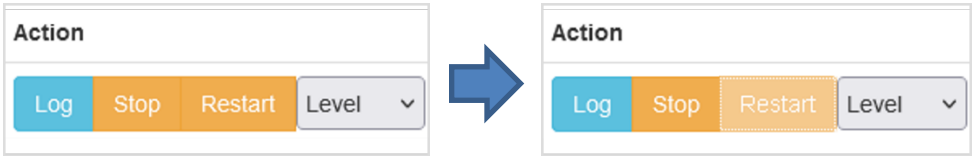
2.4. SYNESIS サービスの再起動

SYNESIS の各種サービスを Management Console から再起動することができます。
サービスによっては、再起動時にキャプチャが停止しますので、ご注意ください。(詳細は「2.4.1.各サービスの役割と再起動時のキャプチャ停止の有無」を参照してください。)
SYNESIS サービスの再起動手順は以下の通りです。

1) Management Console へアクセスします。 ※「3.3.2.1 ログイン」参照
2) 以下の画面が表示されるので、再起動したいサービスの[Restart]ボタンをクリックします。



クリックしたボタンの色が薄い間はサービスの再起動中です。色が元に戻れば再起動は完了です。



2.4.1. 各サービスの役割と再起動時のキャプチャ停止の有無

各サービスの役割は以下の通りです。

サービス名	役割	キャプチャの停止
Tomcat	WEB UI	なし
mvp	各プロセスへの API の提供	なし
NetKeeper	キャプチャ，解析	あり（停止する）
VPEyes	NetKeeper の死活監視(NetKeeper と連動)	
DEService	リアルタイムデコード	なし
FeedService	パケットストアの直接読み出し （ソケットを利用）	なし
Notifier	メールや SNMP Trap などによる通知	なし
CommandAgent	各種スクリプトの実行	なし
SynesisFS	パケットストアの直接読み出し（ファイルシステムを利用） ※初期状態ではサービスは起動していません	なし

NetKeeper を再起動すると実行中のキャプチャは停止します。 再起動後、自動的にキャプチャが再開されるよう設定することが可能です。
詳細は、ユーザガイドの「4.4 キャプチャオプション」の章を参照してください。

2.5. キャプチャカードの再起動

キャプチャカードの状態が異常となった場合、またはキャプチャカードに新しい設定を反映させる場合に、以下の手順に従いキャプチャカードの再起動を行います。

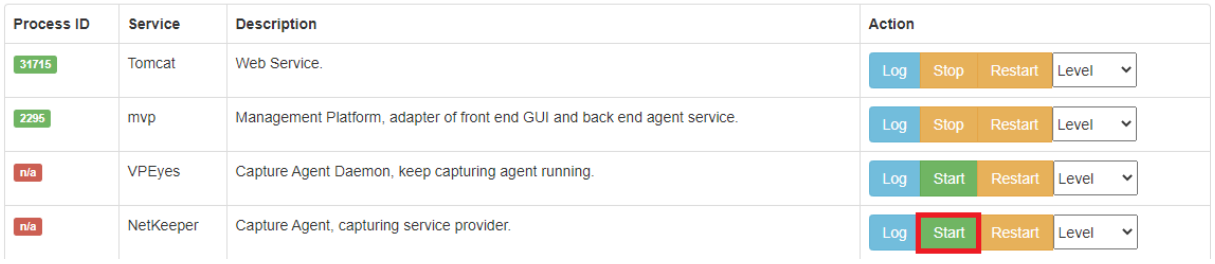
1) SYNESIS のキャプチャおよびリプレイを停止します。
2) Management Console へアクセスします。 ※「3.3.2.1 ログイン」参照
3) 以下の画面が表示されるので、NetKeeper の [Stop]ボタンをクリックします。

4) Netkeeper の Process ID が「n/a」に、[Stop」ボタンが緑の「Start」ボタンに変わったことを確認してください。NetKeeper が停止すると、VPEyes プロセスも同時に停止します。

5) SSH で SYNESIS にログインし、下記のコマンドを実行してキャプチャカードを再起動します。

```
$ sudo service ntservice restart
```

6) SYNESIS の Management Console で、NetKeeper サービスの「Start」ボタンをクリックします。



以上の手順でキャプチャカードが再起動され、SYNESIS が通常通り使用できます。

3. SYNESIS へのアクセス方法

本章では、SYNESIS を運用・管理するのに必要なアクセス方法を説明します。

SYNESIS を構成する主なソフトウェアは以下の通りです。

ソフトウェア		**主な役割**
OS (OS)		OS
SYNESIS ソフトウェア	メイン GUI	パケットキャプチャとその分析、操作 GUI
	Management Console	SYNESIS サービスの操作、ログの確認・収集
iDRAC		ハードウェアのステータスを監視・通知 ※SYNESIS Distributed のみ

詳しい手順については、対応する章を参照してください。

3.1. アクセス方法一覧

SYNESIS を構成するソフトウェアへのアクセス方法は下記の通りです。

アクセス先		**プロトコル**	**開放ポート**	**IP アドレス(デフォルト)** 物理ポート：アドレス	**管理者権限アカウント(デフォルト)**
OS (OS)		RDP	TCP:3389	eno1: 172.22.201.250 eno2-eno4： DHCP	synesis/admin
		SSH	TCP:22		
SYNESIS ソフトウェア	メイン GUI	HTTPS	TCP:443		admin/synesis1
	Management Console				
iDRAC		HTTPS	TCP:443	iDRAC: 192.168.0.120	root/calvin

詳しい手順については、対応する章を参照してください。

3.2. OS

3.2.1. リモートデスクトップ

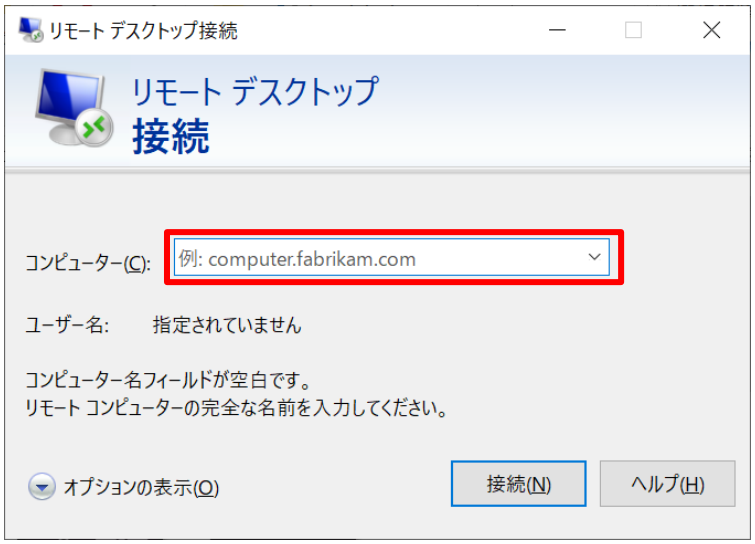
Windows のリモートデスクトップ機能で OS にログインすることができます。

接続は 1 セッションのみです。

3.2.1.1. ログイン

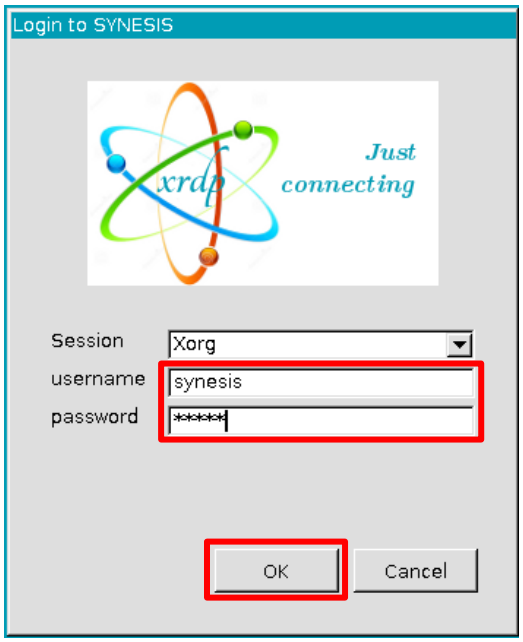
1) Windows のスタートボタンをクリックし、[**すべてのプログラム**] をクリックします。
2) [**アクセサリ**] をクリックし、メニューを展開します。

3) [**リモートデスクトップ接続**] をクリックしてください。以下の画面が表示されます。



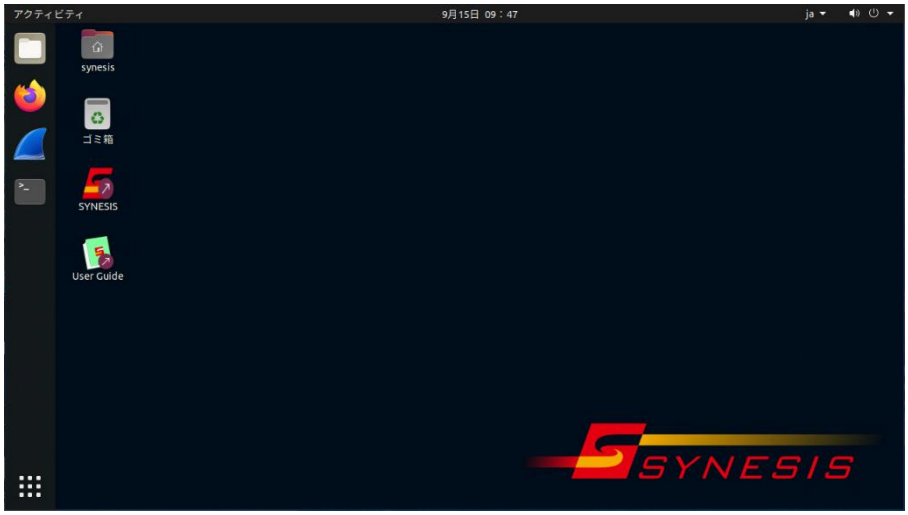
4) [**コンピュータ(C)**]の欄に SYNESIS の管理ポートの IP アドレスを入力して、[**接続**]ボタンをクリックします。
信頼や接続の確認画面が表示された場合は「接続」もしくは「はい」をクリックし接続します。

5) 接続に成功すると、下記のログイン画面が表示されます。
[**Session**] 欄は "Xorg" を選択し、OS のユーザ名とパスワードを [**username**] 欄、[**password**] 欄それぞれに入力します。



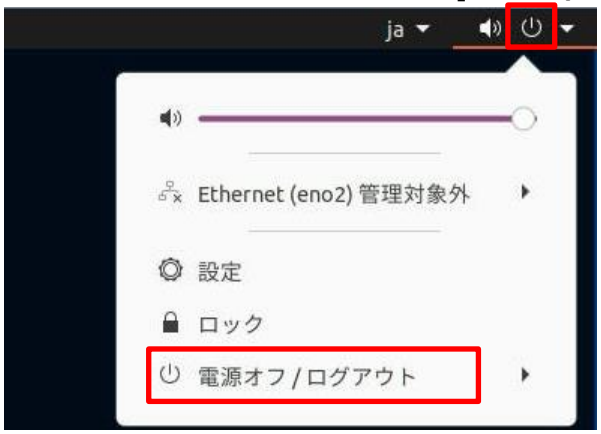
6) 入力後、[**OK**]ボタンをクリックします。

7) ログインに成功すると、OS のデスクトップ画面が表示されます。



3.2.1.2. ログアウト

1) デスクトップ画面右上のボタンをクリックし、[**電源オフ/ログアウト**] をクリックします。



2) [**ログアウト**] をクリックします。

3) 確認ダイアログで [**ログアウト**] をクリックします。
自動ログアウトのカウントダウンもされており、表示されている時間が経過すれば何もしなくても自動でログアウトされます。

3.2.2. SSH

SSH クライアント接続で OS にログインすることができます。

3.2.2.1. ログイン

1) SSH クライアントにて SYNESIS 管理ポートの IP アドレスへアクセスします。
2) ユーザ名、パスワードを入力しログインします。

3.2.2.2. ログアウト

コマンドライン上で「***exit***」コマンドを入力し、ログアウトします。

3.3. SYNESIS ソフトウェア

SYNESIS には Web ブラウザを用いてアクセスします。

3.3.1. メイン GUI

3.3.1.1. サインイン

1) 下記のアドレスを Web ブラウザのアドレスバーに入力すると、SYNESIS にアクセスできます。
https://<*SYNESIS IP Address*>/
2) 以下の画面が表示されるので、SYNESIS アカウントのユーザ名、パスワードを入力して、「サインイン」ボタンをクリックします。

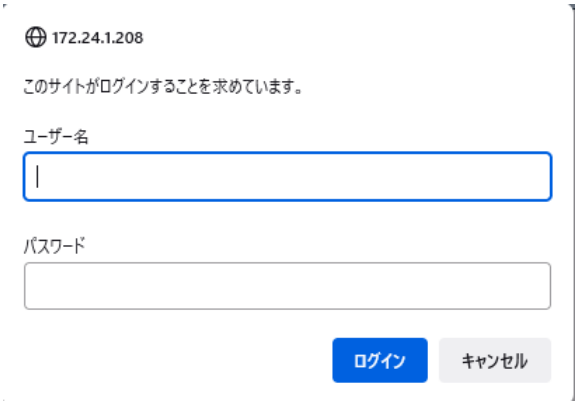
3.3.1.2. サインアウト

ツールバー右上の**[サインアウト]**ボタン  をクリックします。
サインアウトを行うと、サインイン画面に戻ります。

3.3.2. Management Console

3.3.2.1. ログイン

1) 下記のアドレスを Web ブラウザのアドレスバーに入力します。
   https://<*SYNESIS IP address*>/mgmt/
2) 以下の画面が表示されるので、Management Console 用アカウントのユーザ名、パスワードを入力して、[**OK**]ボタンをクリックしてください。



3.3.2.2. ログアウト

ブラウザの本ページを閉じます。

3.4. iDRAC

SYNESIS Distributed をご利用の場合、iDRAC (integrated Dell Remote Access Controller)でサーバのリモート管理を行うことができます。SYNESIS Portable では本機能をご利用いただけません。
なお、iDRAC には Web ブラウザを用いてアクセスします。

3.4.1. ログイン

1) 下記のアドレスを Web ブラウザのアドレスバーに入力すると、iDRAC にアクセスできます。
https://<*iDRAC IP Address*>/
2) 以下ようなのログイン画面が表示されます。

3) ユーザ名、パスワードを入力し[**ログイン**]ボタンをクリックしてください。

3.4.2. ログアウト

1) 画面右上の をクリック後 [**ログアウト**] ボタンをクリックします。

4. 設定の変更

本章では、SYNESIS を構成する各ソフトウェアのアカウントやネットワーク設定などを、必要に合わせて初期設定から変更するための手順を解説します。

4.1. OS の設定変更

4.1.1. ホスト名

ホスト名を変更する場合は、以下の手順を実施します。
なお、ホスト名に関する制限は以下の通りです。

項目	制限
ホスト名文字数	最大 15 文字
ホスト名文字列	アルファベット(A-Z, a-z) 数字(0-9) ハイフン(-) 先頭文字はアルファベット、末尾はハイフン以外

1) SYNESIS のローカルから Terminal を起動するか、リモートから SSH で接続します。
※「3.2.2 SSH」参照

2) 以下の 2 つのコマンドを入力します。

```
$ sudo sed -i -e '1s/.*/<new hostname>/g' /etc/hostname
$ sudo sed -i -e '/127.0.1.1/ c 127.0.1.1\t<new hostname>' /etc/hosts
```

3) 以下の 2 つのコマンドを入力し、出力結果を確認します。

```
$ cat /etc/hostname
<new hostname>
$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 <new hostname>
```

4) OS を再起動します。 ※「2.3 OS の再起動」参照

4.1.2. 管理者アカウント (ユーザ名・パスワード)

ユーザ名の変更には、変更するアカウント以外で管理者権限を持つアカウントが必要です。
初期設定では、管理者権限を持つアカウントは 1 つしかないため、一時的なアカウントを作成してから変更を行います。
手順は、以下の通りです。

1) SYNESIS のローカルから Terminal を起動するか、リモートから SSH で接続します。
※「3.2.2 SSH」参照

2) 下記コマンドを入力し、管理者権限を持つ一時的なアカウントを作成します。
※「5.1.1 OS のアカウント作成」参照

```
$ sudo adduser <username for temporary account>
$ sudo usermod -G sudo <username for temporary account>
```

3) OS を再起動します。 ※「2.3 OS の再起動」参照

4) 「5.1.2 OS のアカウント変更」の手順に従い、ユーザ名とパスワードを変更します。

5) 変更後の管理者アカウントでログイン後、下記コマンドを入力し、管理者権限を持つ一時的なアカウント *<temp user>*を削除します。

```
$ sudo userdel -r <username for temporary account>
```

このとき以下のメッセージが表示されますが、特に問題はありません。

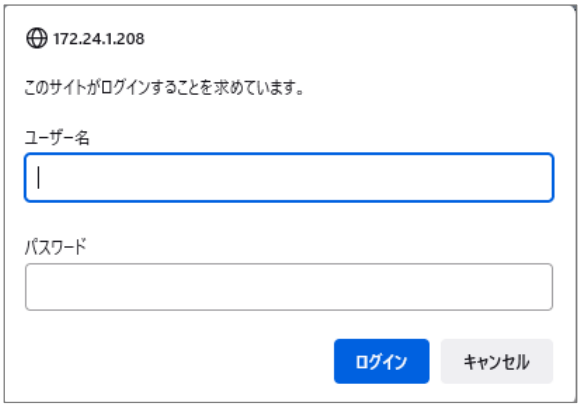
```
userdel: temp のメールスプール (/var/mail/temp) がありません
```

4.1.3. 管理ポートのネットワーク設定 (GUI で設定する方法)

管理ポートの IPv4 のネットワーク設定を GUI で設定する方法は、以下の通りです。
なお、次章「4.1.4 管理ポートのネットワーク設定 (ファイルを編集する方法)」でボンディングインタフェースを設定した場合や IPv6 アドレスを設定した場合は、本設定方法は使用できなくなりますのでご注意ください。

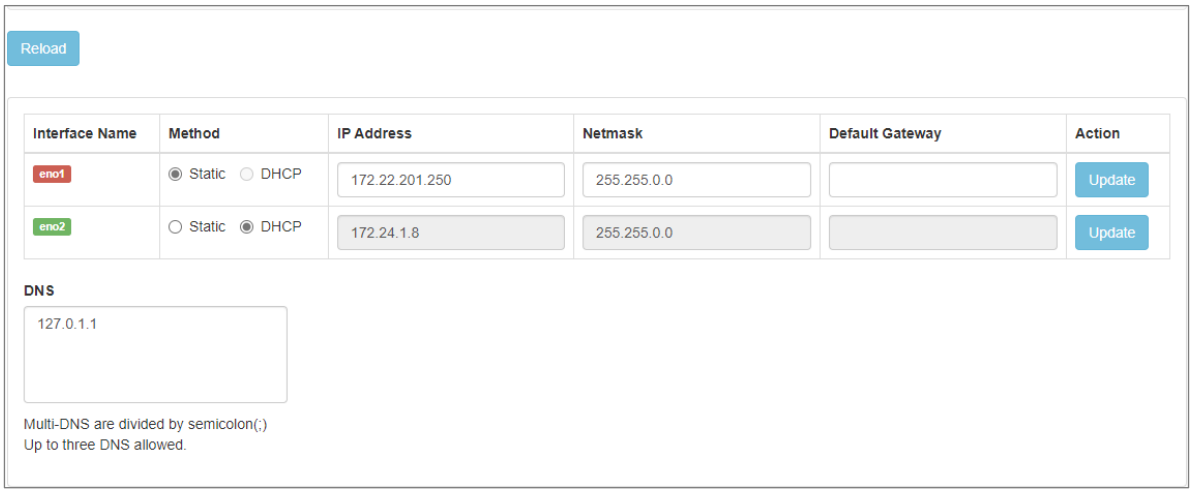
1) 下記のアドレスを Web ブラウザのアドレスバーに入力します。
https://< *SYNESIS IP Address*>/mgmt/

2) 以下の画面が表示されるので、管理者権限を持った SYNESIS アカウントのユーザ名、パスワードを入力して、 [OK]ボタンをクリックしてください。
※「3.3.2. Management Console」の「3.3.2.1 ログイン」参照



3) Management Console が表示されます。画面上部の[Network (IPv4)]タブをクリックします。

4) ネットワーク設定画面に遷移し、現在の設定が表示されます。(下図は 2 ポートの例です)



5) 本画面の操作方法は、以下の通りです。
- [Reload]ボタンをクリックすると、現在の編集内容を破棄してネットワーク設定を再取得します。
- リンクアップしているポートは Interface Name が緑色で、リンクダウンしているポートは赤色で表示されます。
- 固定の IPv4 アドレスを設定する場合は、Method の「Static」を選択し、IP アドレス、マスク、ゲートウェイを入力します。「Update」ボタンをクリックすると、入力した内容が netplan のコンフィグレーションに反映され、新しいネットワーク設定が適用されます。また、管理画面は新しいアドレスにリダイレクトします。
- DHCP に設定する場合は、Method の「DHCP」を選択します。「Update」ボタンをクリックすると、netplan のコンフィグレーションから該当するインタフェースの定義が削除され、新しいネットワーク設定が適用されます。DHCP の場合は新しいアドレスにはリダイレクトしません。
- 全ポートに共通の DNS を設定する場合は、DNS の枠内のアドレスを編集して、リンクアップしているインタフェースの [Update] ボタンをクリックします。入力した DNS サーバが netplan のコンフィグレーションに nameservers として追加されます。複数の DNS を指定する場合は、セミコロン区切りで入力します。
- 起動直後または「Reload」「Update」を実行後、DNS 枠内には /etc/resolv.conf の nameserver エントリを表示します。

4.1.4. 管理ポートのネットワーク設定 (ファイルを編集する方法)

管理ポートのネットワーク設定をファイルの編集によりで設定する方法は、以下の通りです。
なお、本方法でボンディングインタフェースを設定した場合は、前章「4.1.3 管理ポートのネットワーク設定 (GUI で設定する方法)」は使用できなくなりますのでご注意ください。

1) SYNESIS のローカルから Terminal を起動するか、リモートから SSH で接続します。
※「3.2.2 SSH」参照

2) 下記のコマンドを実行して、netplan のファイル名を調べます。

```
$ ls -al /etc/netplan/
```

以下のような実行結果が表示されます。XX-networkd-all.yaml (XX は 2 桁の数値) が次の手順で編集するファイルになります。

```
total 24
drwxr-xr-x   2 root root  4096 Sep 14 18:05 ./
drwxrwxr-x 150 root root 12288 Sep 15 08:30 ../
-rw-r--r--   1 root root   104 Feb 10  2021 01-network-manager-all.yaml
-rw-r--r--   1 root root   283 Sep 14 19:54 02-networkd-all.yaml
```

3) 前の手順で得られたファイルをエディタ(vi)でオープンします。XX の部分に実際の環境と同じ数値を入れ、以下のコマンドを実行します。

```
$ sudo vi /etc/netplan/XX-networkd-all.yaml
```

4) 以下の記述が表示されます。[i]キーを押して挿入(INSERT)モードに移行します。

```
  ethernets:
    eno1:
      addresses:
      - 172.22.201.250/16
      dhcp4: false
      dhcp6: false
    eno2:
      dhcp4: true
  renderer: networkd
  version: 2
```

5) ネットワーク環境に応じて yaml ファイルを編集します。

例 1 ：eno1 に固定 IPv4 アドレス(172.22.201.200/16)を設定する

```
network:
  ethernets:
    eno1:
      addresses:
      - 172.22.201.200/16
      gateway4: 172.22.254.254
      nameservers:
        addresses:
        - 172.22.254.254
      dhcp4: false
      dhcp6: false
    eno2:
      dhcp4: true
  renderer: networkd
  version: 2
```

eno2 以降のアドレスを変更する場合も、同様にファイルを編集します。

例 2：eno1 に固定 IPv4 アドレス(172.22.201.200/16)と固定 IPv6 アドレス(2001:DB8:1000::1/48)を設定する

```
network:
  ethernets:
    eno1:
      addresses:
      - 172.22.201.200/16
      - 2001:0DB8:1000::1/48
      gateway4: 172.22.254.254
      gateway6: 2001:0DB8:1000::FFFE
      nameservers:
        addresses:
        - 172.22.254.254
      dhcp4: false
      dhcp6: false
    eno2:
      dhcp4: true
  renderer: networkd
  version: 2
```

eno2 以降のアドレスを変更する場合も、同様にファイルを編集します。

例 3：eno1 を DHCP に設定する

```
network:
  ethernets:
    eno1:
      dhcp4: true
      dhcp6: true
    eno2:
      dhcp4: true
  renderer: networkd
  version: 2
```

eno2 以降のアドレスを変更する場合も、同様にファイルを編集します。

例 4：eno1/eno2 をボンディングインタフェース(active-backup モード)で構成し、固定 IPv4 アドレス(172.22.201.200/16)を設定する。

```
network:
  ethernets:
    eno1:
      dhcp4: false
      dhcp6: false
    eno2:
      dhcp4: false
      dhcp6: false
    bonds:
      bond0:
        addresses:
        - 172.22.201.200/16
        gateway4: 172.22.254.254
        nameservers:
          addresses:
          - 172.22.254.254
        interfaces: [eno1, eno2]
        parameters:
          mode: active-backup
          primary: eno1
          mii-monitor-interval: 100
  renderer: networkd
  version: 2
```

6) 設定を変更しましたら、<Esc>キーを押し、その後「:x」と入力して<Enter>キーを押します。
変更が保存され、エディタが終了します。

7) 下記コマンドを入力し、設定変更を反映します。

```
$ sudo netplan apply
```

4.2. SYNESIS の設定変更

SYNESIS の使用を開始する前に、ご利用の環境に合わせて SYNESIS の設定を変更してください。

4.2.1. Firewall 設定

SYNESIS で使用していないポートは、SYNESIS 上の Firewall にて通信が遮断されています。
SNMP トラップトリガ機能を利用する場合などは、使用するポートを Firewall のルールに追加します。ルールはポートの他、IP アドレスなどでも設定が可能です。
SYNESIS で使用するポートは、ユーザガイドの「2.4　使用するポートの一覧」を参照してください。
なお、出荷時は、SYNESIS にアクセスするポート番号の通信のみ許可する設定になっています。

4.2.1.1. Firewall の設定の確認(GUI で確認する方法)

以下の手順で、現在の Firewall の設定を確認できます。

1) Management Console にログインします。※「3.3.2.1 ログイン」参照
2) 画面上部の[Firewall]タブをクリックします。

※表示例

Refresh

IPv4

#	From Address	From Port	To Address	To Port	Protocol	Action	Direction
1	Any	Any	Any	22	Tcp	Allow	In
2	Any	Any	Any	80	Tcp	Allow	In
3	Any	Any	Any	443	Tcp	Allow	In
4	Any	Any	Any	3389	Any	Allow	In
5	Any	Any	Any	1311	Any	Allow	In

IPv6

#	From Address	From Port	To Address	To Port	Protocol	Action	Direction
1	Any	Any	Any	22	Tcp	Allow	In
2	Any	Any	Any	80	Tcp	Allow	In
3	Any	Any	Any	443	Tcp	Allow	In
4	Any	Any	Any	3389	Any	Allow	In
5	Any	Any	Any	1311	Any	Allow	In

4.2.1.2. Firewall の設定の確認(コマンドラインで確認する方法)

以下のコマンドで、現在の Firewall の設定を確認できます。

```
$ sudo ufw status verbose
```

※表示例

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To                         Action      From
--                         ------      ----
22                         ALLOW IN    Anywhere
80                         ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
3389                       ALLOW IN    Anywhere
22 (v6)                    ALLOW IN    Anywhere (v6)
80 (v6)                    ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)
3389 (v6)                  ALLOW IN    Anywhere (v6)
```

4.2.1.3. 許可ルールの追加

現在のルールから新たにルールを追加する手順は、以下の通りです。

1) 以下のコマンドを実行します。

```
$ sudo ufw allow <rule syntax>
```

ルールの指定方法<rule syntax>は、以下のようになっています。

ルールの指定方法	**詳細**
80	80 番ポートを許可
http	http を許可 指定したプロトコルが、/etc/services で規定されている場合のみ有効
80/tcp	TCP 80 番ポートを許可
80,443/tcp	TCP 80 番、443 番ポートを許可
8080:8083/tcp	TCP 8080-8083 番ポートを許可
from 192.168.0.101 to any port 80	192.168.0.101 からのアドレスのみ 80 番ポートを許可
from 192.168.1.0/24 to any port 80	192.168.1.0/24 からのアドレスのみ 80 番ポートを許可

2) 4.2.1.2 章に従い、手順 3)で指定したルールが追加されていることを確認します。

3) 以下のコマンドを実行します。

```
$ sudo systemctl restart ufw
```

よくある設定については、**4.2.1.5 設定例**に記載しましたので、参照してください。

4.2.1.4. 許可ルールの削除

現在のルールを削除する手順は、以下の通りです。

1) 以下のコマンドを実行します。

```
$ sudo ufw status numbered
```

2) 以下のような結果が得られますので、削除するルールの最左列の番号を控えておきます。

```
To                         Action      From
--                         ------      ----
[ 1] 22                    ALLOW IN    Anywhere
[ 2] 80                    ALLOW IN    Anywhere
[ 3] 443                   ALLOW IN    Anywhere
[ 4] 3389                  ALLOW IN    Anywhere
[ 5] 162                   ALLOW IN    Anywhere
[ 6] 22 (v6)               ALLOW IN    Anywhere (v6)
[ 7] 80 (v6)               ALLOW IN    Anywhere (v6)
[ 8] 443 (v6)              ALLOW IN    Anywhere (v6)
[ 9] 3389 (v6)             ALLOW IN    Anywhere (v6)
[10] 162 (v6)              ALLOW IN    Anywhere (v6)
```

3) 手順 2)で控えた番号で、大きい数値から順番に以下のコマンドを繰り返します。

```
$ sudo ufw delete <The number listed in the leftmost column>
```

以下の記述は、2)の結果からポート番号 162 を遮断する場合の例です。

```
$ sudo ufw delete 10
Deleting:
allow 162 (v6)
Proceed with operation (y|n)? y <-間違いがなければ”y”を入力
Rule deleted
$ sudo ufw delete 5
Deleting:
allow 162
Proceed with operation (y|n)? y <-間違いがなければ”y”を入力
Rule deleted
```

4) 4.2.1.2 章に従い、手順 3)で指定したポートが削除されていることを確認します。

5) 以下のコマンドを実行します。

```
$ sudo systemctl restart ufw
```

4.2.1.5. 設定例

[出荷時の設定から特定のポートを追加で許可する場合]

現在のルールから特定ポートの通信を許可する場合の手順は、以下の通りです。

SNMP トラップを SYNESIS に受信させる場合などは、こちらの設定を実施します。

以下の例は、現在の設定から、162 番ポートを追加する場合の設定方法です。

1) 以下のコマンドを実行します。

```
$ sudo ufw allow 162
```

2) 以下のコマンドで手順 1)で指定したポートが追加されていることを確認します。

```
$ sudo ufw status
状態: アクティブ

To                         Action      From
--                         ------      ----
22                         ALLOW IN    Anywhere
80                         ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
3389                       ALLOW IN    Anywhere
1311                       ALLOW IN    Anywhere
162                        ALLOW IN    Anywhere
22 (v6)                    ALLOW IN    Anywhere (v6)
80 (v6)                    ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)
3389 (v6)                  ALLOW IN    Anywhere (v6)
1311 (v6)                  ALLOW IN    Anywhere (v6)
162 (v6)                   ALLOW IN    Anywhere (v6)
```

3) 以下のコマンドを実行し、設定を反映します。

```
$ sudo systemctl restart ufw
```

[特定の IP アドレスからの通信のみ SYNESIS の使用しているポートに対して許可する場合]
IP アドレスとポート番号の組み合わせで通信を許可する場合は、一旦現在のルールを削除し、IP アドレスとポート番号の組み合わせのルールを追加します。
以下の例は、192.168.1.0/24 からの通信のみ許可する場合の設定方法です。

1) 以下のコマンドを実行し、Firewall を無効化して設定をリセットします。

```
$ sudo ufw reset
```

このとき以下のメッセージが表示されますので、“y”と入力します。

```
インストール時のデフォルトルールを再設定します。既存の SSH 接続を中断することがあります。
操作を続行しますか (y|n)? y   <- “y”と入力
'before.rules'から'/etc/ufw/before.rules.20211208_131358'にバックアップしています
'after.rules'から'/etc/ufw/after.rules.20211208_131358'にバックアップしています
'before6.rules'から'/etc/ufw/before6.rules.20211208_131358'にバックアップしています
'user6.rules'から'/etc/ufw/user6.rules.20211208_131358'にバックアップしています
'after6.rules'から'/etc/ufw/after6.rules.20211208_131358'にバックアップしています
'user.rules'から'/etc/ufw/user.rules.20211208_131358'にバックアップしています
```

2) リモートで接続している場合は、まず SSH で使用する 22 番ポートを許可します。ローカルで接続している場合は、本手順は不要です。

```
$ sudo ufw allow 22
```

3) Firewall を有効にします。

```
$ sudo ufw enable
```

このとき以下のメッセージが表示されますので、“y”を選択します。

```
Command may disrupt existing ssh connections. Proceed with operation (y|n)?
```

リモートで接続している場合は、SSH が切断されますので SSH の再接続を行います。

4) IP アドレスとポート番号の組み合わせのルールを追加します。

SYNESIS で使用するポートは、ユーザガイドの「2.4 使用するポートの一覧」を参照してください。以下は、192.168.1.0/24 から 22、80、443、3389、1311 番ポートを許可する場合のコマンドです。

```
$ sudo ufw allow from 192.168.1.0/24 to any port 22
$ sudo ufw allow from 192.168.1.0/24 to any port 80
$ sudo ufw allow from 192.168.1.0/24 to any port 443
$ sudo ufw allow from 192.168.1.0/24 to any port 3389
$ sudo ufw allow from 192.168.1.0/24 to any port 1311
```

5) 以下のコマンドで、手順 2)と 4)で指定したルールが追加されていることを確認します。

```
$ sudo ufw status
状態: アクティブ

To                         Action      From
--                         ------      ----
22                         ALLOW IN    Anywhere
22                         ALLOW IN    192.168.1.0/24
80                         ALLOW IN    192.168.1.0/24
443                        ALLOW IN    192.168.1.0/24
3389                       ALLOW IN    192.168.1.0/24
1311                       ALLOW IN    192.168.1.0/24
22 (v6)                    ALLOW IN    Anywhere (v6)
```

6) 手順 2）で指定した設定を削除します。SSH で許可されていない IP アドレスから設定を行なっている場合、以下のコマンドを入力するとその後一切 SSH で接続できなくなりますのでご注意ください。

```
$ sudo ufw delete allow 22
```

7) 以下のコマンドで、手順 4)で指定したルールのみが追加されていることを確認します。

```
$ sudo ufw status
状態: アクティブ

To                         Action      From
--                         ------      ----
22                         ALLOW IN    192.168.1.0/24
80                         ALLOW IN    192.168.1.0/24
443                        ALLOW IN    192.168.1.0/24
3389                       ALLOW IN    192.168.1.0/24
1311                       ALLOW IN    192.168.1.0/24
```

8) 以下のコマンドを実行し、設定を反映します。

```
$ sudo systemctl restart ufw
```

4.2.2. SSL/TLS サーバ証明書の変更

SYNESIS は、v4.0 より SSL/TLS 通信となっています。SSL/TLS 通信に用いる自己証明書を出荷時に添付しています。これを任意の証明書に変更することが可能です。
証明書を変更する場合は、以下の手順を実施してください。変更しない場合は、本手順は不要です。

- 注意事項
  - CA 証明書、サーバ証明書、及びサーバの秘密鍵の 3 つが必要です。
  - 証明書の作成手順については環境により複数の方法があるため、必要な場合はお客様のシステム、又はネットワーク管理者へお問い合わせください。
  - 証明書と秘密鍵は PEM 形式(拡張子:.pem)、または DER 形式(拡張子:.cer,.der)である必要があります。

1) 用意した証明書と秘密鍵を ”/etc/nginx/synesis” にコピーします。
   ※以下のファイル名で手順を記載します。
   - CA 証明書: dummy_ca.pem
   - サーバ証明書: dummy_server.pem
   - サーバの秘密鍵: dummy_serverkey.pem
2) vi 等のテキストエディタで “/etc/nginx/synesis/synesis.conf” を開き、以下の変更を行います。
   - "ssl_catificate"の右側のパスを「サーバ証明書」のパスに修正
   - "ssl_catificate_key"の右側のパスを「サーバの秘密鍵」のパスに修正
   - "ssl_trusted_catificate"の右側のパスを「CA 証明書」のパスに修正

```
$ sudo vi /etc/nginx/synesis/synesis.conf
# Settings for SYNESIS

# SSL/TLS Settings
ssl_certificate      /etc/nginx/synesis/dummy_server.pem;
ssl_certificate_key  /etc/nginx/synesis/dummy_serverkey.pem;
ssl_trusted_certificate     /etc/nginx/synesis/dummy_ca.pem;
ssl_dhparam          /etc/nginx/synesis/dhparam.pem
```

3) 保存して、テキストエディタを閉じます。vi の場合 “:wq” を入力することで保存ができます。
4) 以下のコマンドを入力し、エラーが無いことを確認します。

```
$sudo nginx -t
```

5) 以下のコマンドを入力して、設定の再読み込みを行います。

```
$sudo nginx -s reload
```

4.2.3. IPv6 アドレスによる HTTPS アクセスの許可

SYNESIS に対して IPv6 アドレスを使用してメイン GUI や Management Console にアクセスすることが可能です。
IPv6 アドレスを使用してのアクセスを許可する場合は、以下の手順を実施してください。

1) vi 等のテキストエディタで “/etc/nginx/synesis/synesis.conf” を開き、全 IPv6 アドレスの 443 ポートへのアクセスを許可する設定を追加します。

```
$ sudo vi /etc/nginx/synesis/synesis.conf
# SSL/TLS Web Service
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    client_max_body_size 0;
```

2) 保存して、テキストエディタを閉じます。vi の場合 “:wq” を入力することで保存ができます。

3) 以下のコマンドを入力し、エラーが無いことを確認します。

```
$sudo nginx -t
```

4) 以下のコマンドを入力して、設定の再読み込みを行います。

```
$sudo nginx -s reload
```

4.2.4. NTP サーバ

NTP サーバの設定方法は、ユーザガイドの「16. 時刻同期」を参照してください。

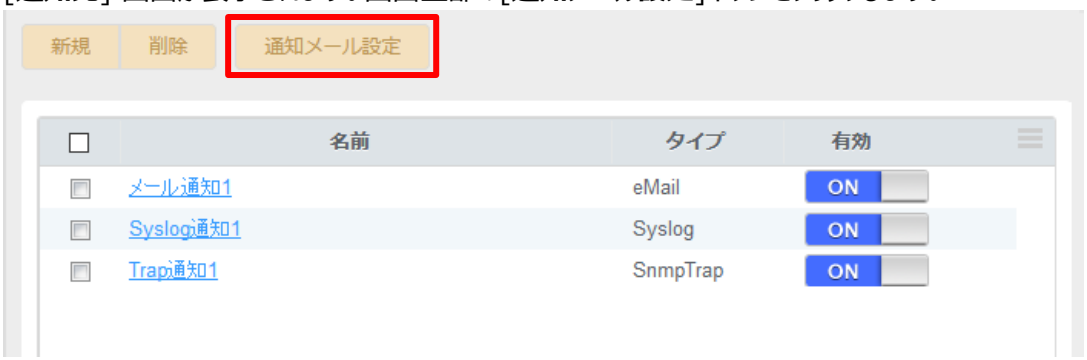
4.2.5. SMTP サーバ

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照

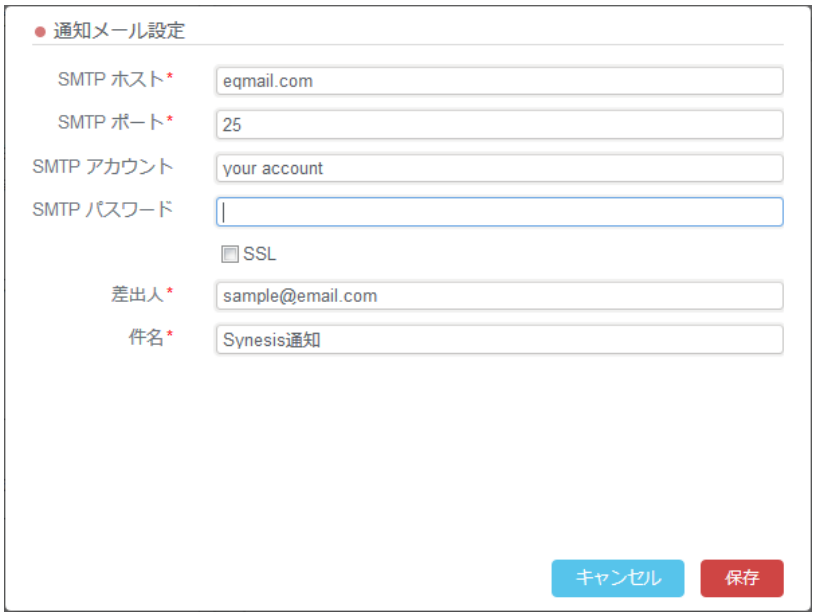
2) サインインしたトップ画面の右側上部にある構成アイコン をクリックしてください。

3) [**構成**] 画面が表示されます。左側のメニュー [**構成**] >[**アラートと通知**] >[**通知先**] をクリックします。

4) [**通知先**] 画面が表示されます。画面上部の[**通知メール設定**]ボタンをクリックします。



5) [**通知メール設定**] 画面が表示されます。SMTP サーバや通知メールに関する設定を変更して、[**保存**]ボタンをクリックします。



4.2.6. CIFS を使用したストレージ共有

大容量のネットワークストレージをトレースファイル等大きいファイルの格納先とする場合、CIFS(Common Internet File System)クライアントを使用してそのストレージをマウントすることができます。
ネットワークストレージのマウントは以下手順を実施してください。なお、本手順を実施する前に、CIFS サーバが正しくセットアップされ TCP 445 番ポートの受信が許可されていることを確認してください。

1) SYNESIS のローカルから Terminal を起動するか、リモートから SYNESIS へ SSH で接続します。
※「3.2.2 SSH」参照

2) マウント先のディレクトリを作成します。

```
$ sudo mkdir -m 0755 -p dest-directory
```

3) 作成したディレクトリへネットワークストレージをマウントします。

```
$ sudo mount -t cifs -o
username=username,password=password,uid=uid,gid=gid,file_mode=0644,dir_mode=0755 //remote-address/remote-shared-directory dest-directory
```

以下に CIFS サーバ 192.0.2.100 の shared ディレクトリを、/mnt/remote ディレクトリにマウントする例を示します。

```
$ sudo mkdir -m 0755 -p /mnt/remote
$ sudo mount -t cifs -o username=user,password=pass,uid=`id -u`,gid=
`id -g`,file_mode=0644,dir_mode=0755 //192.0.2.100/shared /mnt/remote
```

username/password は CIFS サーバで設定したユーザ情報を指定してください。またマウントしたディレクトリへのアクセスを root のみに限定する場合は、uid/gid を省略しても構いません。

4.3. iDRAC の設定変更

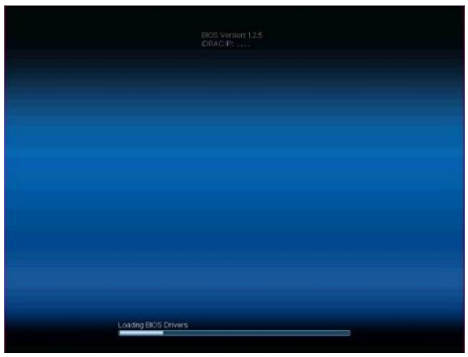
4.3.1. iDRAC ポートのネットワーク設定

iDRAC の IP アドレスが不明である場合や、iDRAC ポートがネットワークに接続されていない場合は、機器に直接接続されたコンソールを利用して iDRAC のネットワーク設定を行ってください。
それらに該当しない場合は、リモートから iDRAC のネットワーク設定を行うことが可能です。

4.3.1.1. ローカルコンソールからの設定

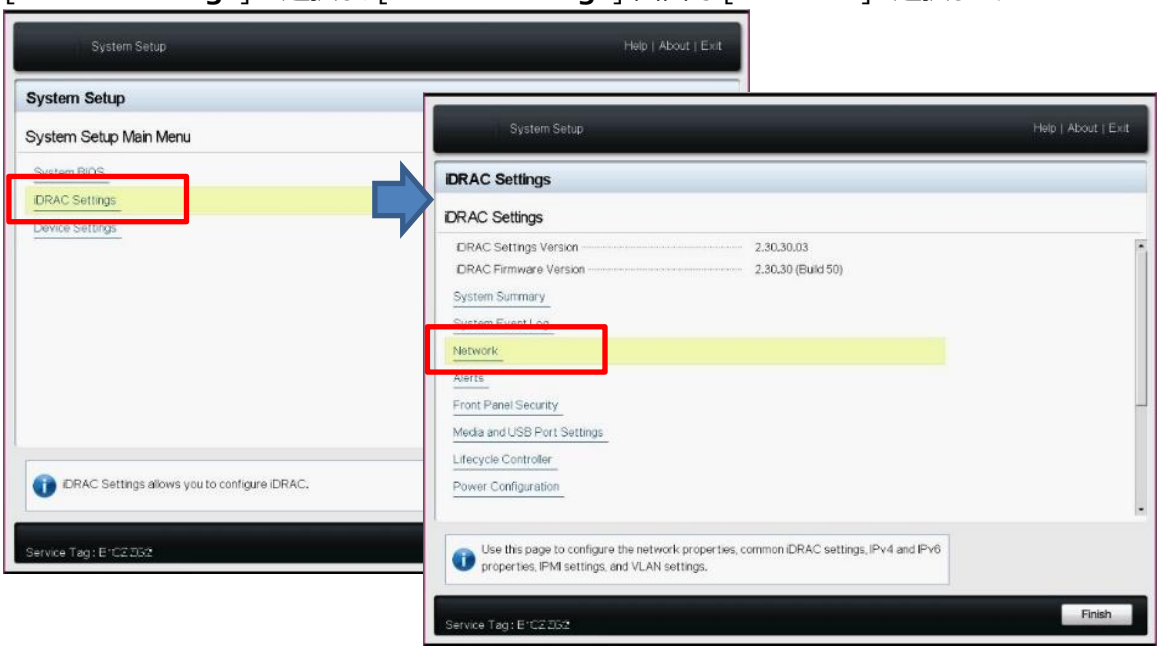
ローカルコンソールからの iDRAC のネットワーク設定の変更手順は、以下の通りです。

1) SYNESIS を起動、または再起動します。 ※「2.1 起動」または「2.3 OS の再起動」参照
2) 以下のような画面が表示されます。

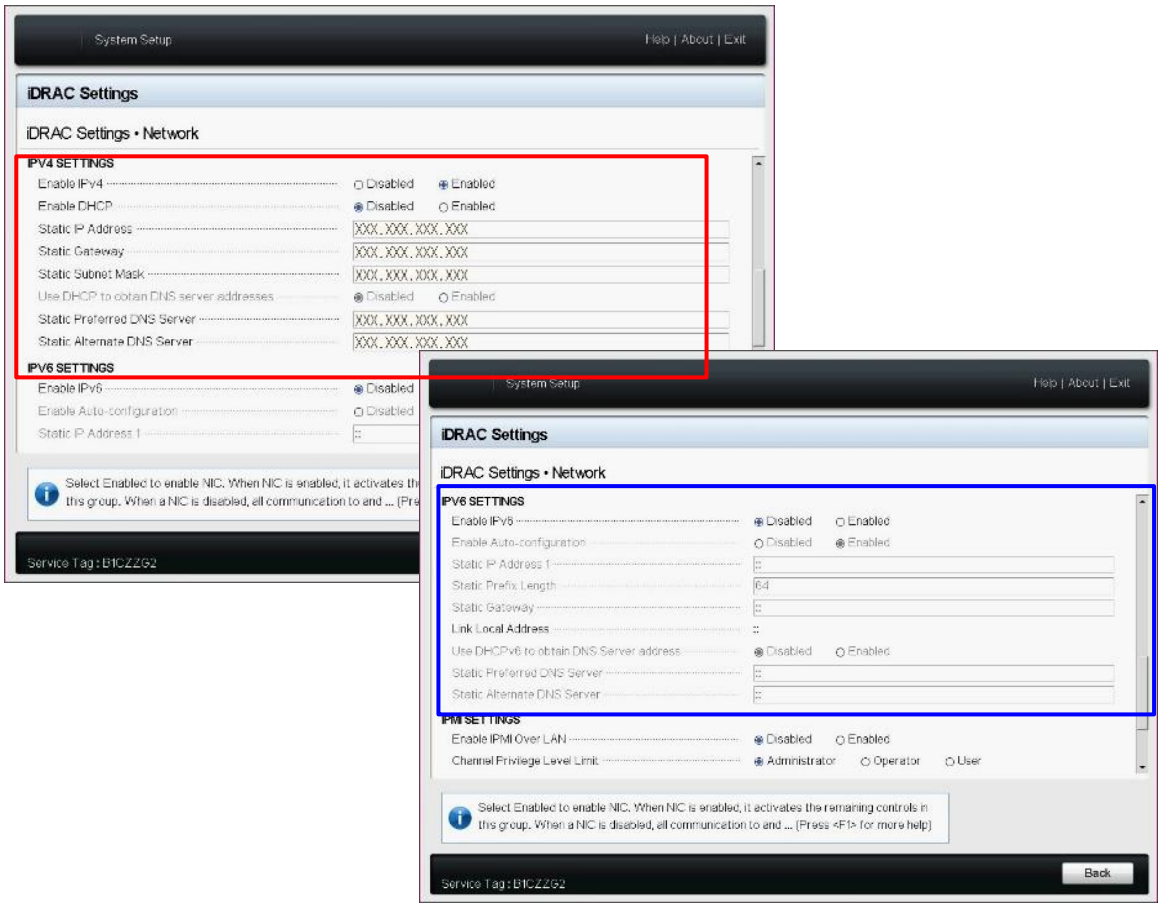


3) 画面上部に以下のような表示が現れたら、キーボードの「F2」を押下します。

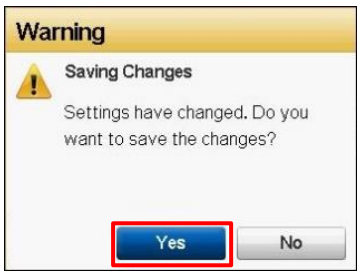
4) 以下のような [**System Setup**] 画面が表示されます。
[**iDRAC Settings**] を選択し、[**iDRAC Settings**] 画面で [**Network**]を選択します。

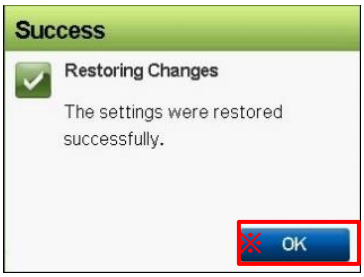


5) [**iDRAC Settings･Network**]画面より、[**IPv4 SETTINGS**](**赤枠**)または[**IPv6 SETTINGS**] (**青枠**)の設定を変更し、変更後に右側上部にある＜**Exit**＞をクリックします。



6) 以下の画面が表示されますので、[**Yes**]をクリックします。
変更を取り消す場合は、[**Saving Changes**] 画面で[**No**]をクリックし、[**Restoring Changes**]画面で[**OK**]をクリックします。





7) [**System Setup**] 画面まで戻りますので、右側上部にある[**Exit**]をクリックします。
以下の画面が表示されましたら[**Yes**]をクリックしてください。

以上で設定は完了です。必要に応じて iDRAC へログインできることを確認してください。

4.3.1.2. リモートからの設定

1) iDRAC にログインします。 ※「3.4.1 ログイン」参照

2) 画面の上部にあるメニューより [**iDRAC 設定**] >[**接続性**] をクリックします。

3) [**ネットワーク**] >[**IPv4 設定**] または [**IPv6 設定**] にて設定を変更して[**適用**]をクリックします。

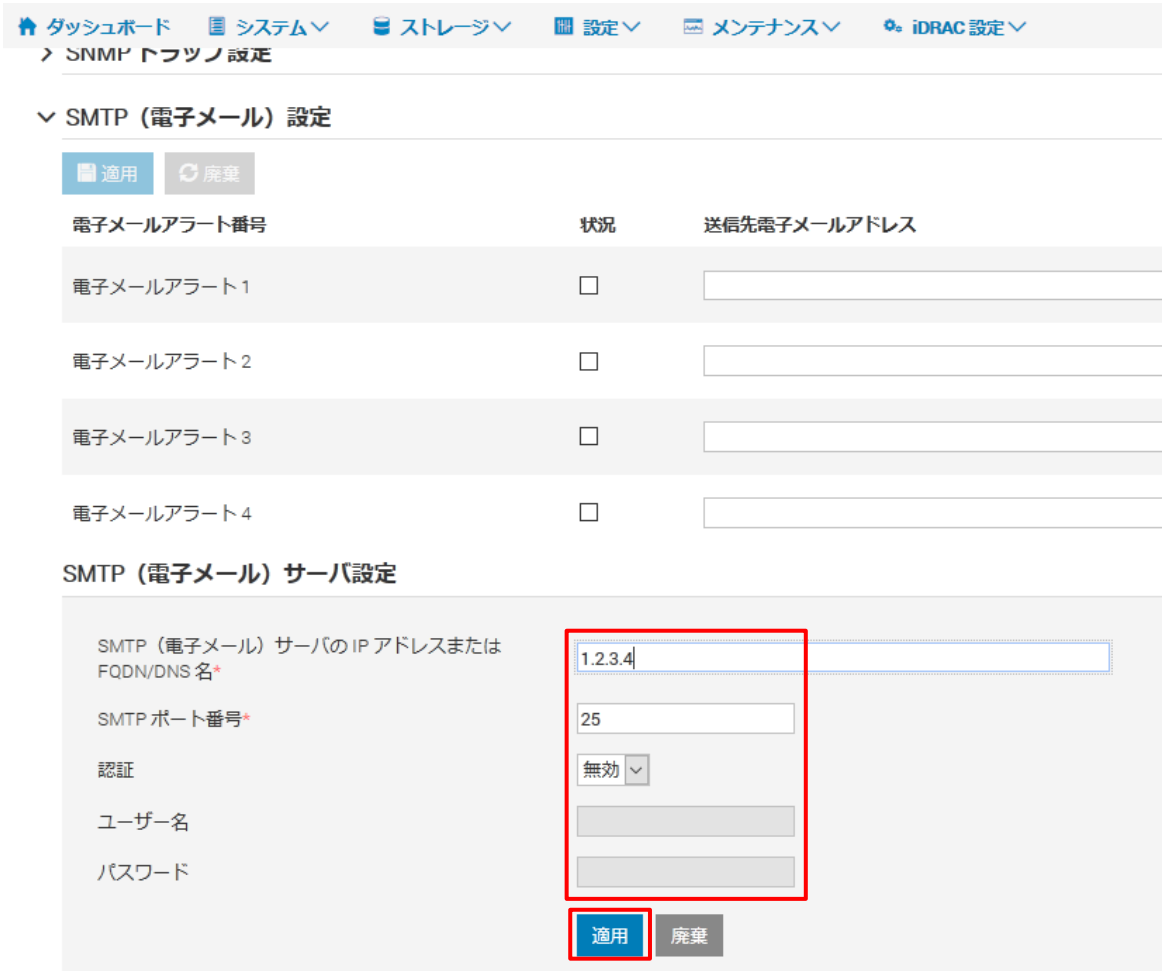
4) アクセス制限の設定をする場合は、[**ネットワーク**]>[**拡張ネットワーク設定**]>[**ネットワークセキュリティ**]にて[**IP 範囲有効**]を有効に変更し、アクセスを許可したい IP アドレス範囲を[**IP 範囲アドレス**]、[**IP 範囲サブネットマスク**]に入力して[**適用**]をクリックします。

4.3.2. SMTP サーバの設定

iDRAC からのアラートをメールで通知する場合は、SMTP サーバの設定を行ってください。
SMTP 以外のアラート通知については「6.1. iDRAC：ハードウェアの監視」を参照してください。

1) iDRAC にログインします。 ※「3.4.1 ログイン」参照
2) 画面の上部にあるメニューより[設定]>[システム設定]をクリックします。

3) 「SNMP(電子メール)設定」の「SMTP(電子メール)サーバ設定」にて設定を変更し、画面下部にある[適用]をクリックします。



5. アカウント管理

本章では、SYNESIS を運用するのに必要なアカウントの管理方法を説明します。
SYNESIS を構成する 3 つのシステム、OS と SYNESIS、 iDRAC(portable は含まない)に対して、各々アカウントを作成・管理します。

5.1. OS のアカウント

OS のアカウントはローカルの Terminal または SSH から編集することができます。
編集の際には管理者権限のあるユーザでログインしてください。
アカウントに関する制限は以下の通りです。

ユーザ名文字数	16 文字
ユーザ名文字列	アルファベット(a-z)　※大文字は使用不可 数字(0-9) アンダーバー(_) 先頭文字に数字は使用不可
パスワード文字数	16 文字
パスワード文字列	アルファベット(A-Z, a-z) 数字(0-9) 特殊文字(! # $ % & ( ) = - ^ | { } [ ] + * ; : < > , ? _)

5.1.1. OS のアカウント作成

5.1.1.1. アカウントの作成

ユーザを新規追加する場合は、以下のコマンドを入力します。

```
$ sudo adduser <username>
[sudo] password for <Login username>: パスワードを入力
Adding user '<username>' ...
Adding new group '<username>' (1002) ...
Adding new user '<username>' (1002) with group `<username>' ...
Creating home directory '/home/<username>' ...
Copying files from '/etc/skel' ...
Enter new UNIX password: 作成するパスワードを入力
Retype new UNIX password: 作成するパスワードを入力
passwd: password updated successfully
Changing user information for <username>
Enter the new value, or press ENTER for the default
        Full Name []: Name of your choice (not required)      省略可
        Room Number []: Number of your choice (not required)  省略可
        Work Phone []: Number of your choice (not required)   省略可
        Home Phone []: Number of your choice (not required)   省略可
        Other []: Information of your choice (not required)   省略可
Is the information correct? [Y/n] y
```

作成したアカウントに管理者権限を与える場合は、以下のコマンドも入力します。
sudo コマンドが使用できるようになります。

```
$ sudo usermod -G sudo <username>
```

5.1.1.2. デスクトップアイコンの設定

新しく作成したアカウントにはデスクトップアイコンからのアプリケーション起動権限がありません。以下の手順で起動を許可します。

1) 作成した新しいアカウントでログインします。
2) SYNESIS デスクトップアイコンからの起動を許可します。

```
$ gio set Desktop/synesis.desktop "metadata::trusted" true
$ chmod +x Desktop/synesis.desktop
```

3) User Guide デスクトップアイコンからの起動を許可します。

```
$ gio set Desktop/synesis_manual.desktop "metadata::trusted" true
$ chmod +x Desktop/synesis_manual.desktop
```

5.1.2. OS のアカウント変更

5.1.2.1. ユーザ名の変更

ユーザ名の変更には、そのアカウントとは別の、管理者権限を持つアカウントが必要になります。そのようなアカウントがない場合は、「4.1.2 管理者アカウント (ユーザ名・パスワード)」に従って、一時的なアカウントを作成してください。
作成したアカウントでユーザ名の変更を行い、変更後に作成したアカウントを削除します。

1) 変更したいアカウント以外の管理者権限を持つアカウントでログインします。
2) ユーザ名を変更するには、以下のコマンドを入力します。
   変更前のユーザ：username before change
   変更後のユーザ: username after change

```
$ sudo usermod -l <username after change> <username before change>
$ sudo groupmod -n <username after change> <username before change>
$ sudo usermod -d /home/<username after change> -m <username after change>
$ sudo usermod -c <username after change>,,, <username after change>
```

※以下のファイルで当該アカウントの設定の変更を確認できます。

- /etc/passwd
- /etc/group

3) 下記コマンドを実行し、Firefox の古い設定ファイルを削除します。

```
$ cd /home/<username after change>
$ sudo find .mozilla -name addonStartup.json.lz4 | xargs rm
```

4) 下記コマンドを実行し、Firefox 設定ファイルのユーザ名を書き換えます。

```
$ sudo find .mozilla -name extensions.json | xargs -o sed -i -e
"s/\/home\/<username before change>/\/home\/<username after change>/g"
```

5) OS を再起動します。 ※「2.3 OS の再起動」参照
6) 変更されたアカウントでログインし、ログイン方法に応じて下記の手順を行います。
7) ユーザ名変更のために、一時的なアカウントを作成している場合は、「5.1.3 OS のアカウント削除」の手順で当該アカウントを削除します。
8) OS を再起動します。 ※「2.3 OS の再起動」参照

※「3.2.1.1 ログイン」の手順により変更後のユーザ名で OS へログインし Firefox を初回起動した際に、Firefox の画面に乱れが発生する可能性があります。その場合、Firefox を再起動することで正常に回復します。

5.1.2.2. パスワードの変更

ユーザパスワードを変更する場合は、以下のコマンドを入力します。

```
$ sudo passwd <username>
[sudo] password for <login username>: パスワードを入力
Enter new UNIX password: 変更するパスワードを入力
Retype new UNIX password: 変更するパスワードを入力
passwd: password updated successfully
```

5.1.3. OS のアカウント削除

ユーザを削除する場合は、以下のコマンドを入力します。

```
$sudo userdel -r <username>
[sudo] password for <login username>: パスワードを入力
```

下記の行が出力されますが、正常動作ですので問題ありません。

```
userdel: <username>のメールスプール (/var/mail/xxx) がありません
```

5.2. SYNESIS のアカウント

SYNESIS のアカウントには 2 種類あります。ひとつはメイン GUI 用のアカウントで、キャプチャの実行や分析が行える操作用アカウントになります。もうひとつは Management Console 用のアカウントで、SYNESIS サービスの操作やログの確認・収集が行えます。
アカウントの作成・管理方法はそれぞれのリンク先を参照してください。

5.2.1. メイン GUI

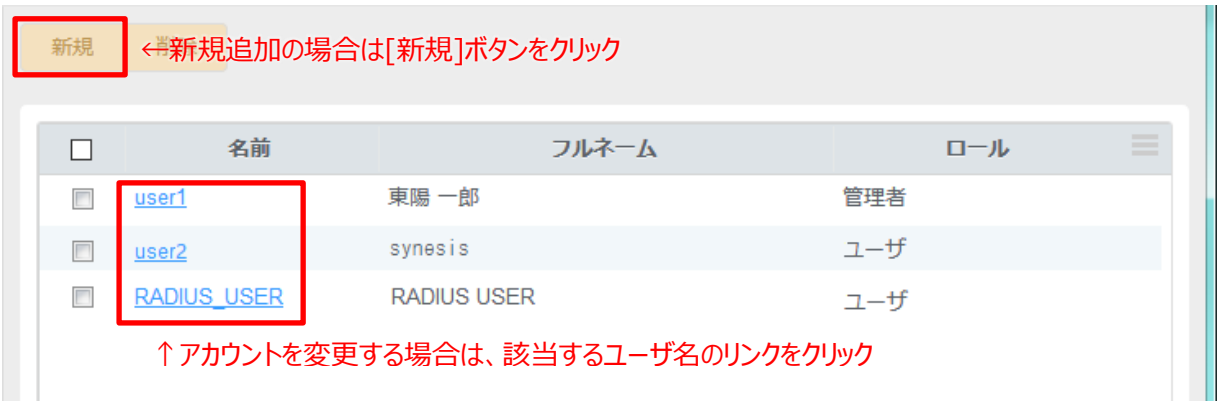
SYNESIS に管理者アカウントでサインインしてください。
サインイン後、ツールバー上の構成アイコン をクリックしてください。
構成メニューの [**システム**]>[**ユーザ**] から、SYNESIS のアカウントの作成・管理が行えます。

アカウントに関する制限は以下の通りです。

同時セッション数	3(デフォルト)
ユーザ名, 姓, 名 文字数	50 文字（50 バイト）以下
ユーザ名, 姓, 名 文字列	下記が利用不可 ! # $ % & = ~ ^ | ¥ ` @ + * , ? (半角) ！ ＃ ＄ ％ ＆ ＝ ～ ＾ ｜ ¥ ‘ @ ＋ ＊ 、 。 ？ (全角)
パスワード文字数	30 文字（30 バイト）以下
パスワード文字列	下記が利用不可 ! # $ % & = ~ ^ | ¥ ` @ + * , ? (半角) ！ ＃ ＄ ％ ＆ ＝ ～ ＾ ｜ ¥ ‘ @ ＋ ＊ 、 。 ？(全角)
ロール	管理者：制限なし ユーザ：主に解析・閲覧機能のみ利用可能 各ロールでできる操作の詳細は、ユーザガイドの「15. ユーザと認証」を参照してください。

5.2.1.1. SYNESIS メイン GUI のアカウント作成・変更

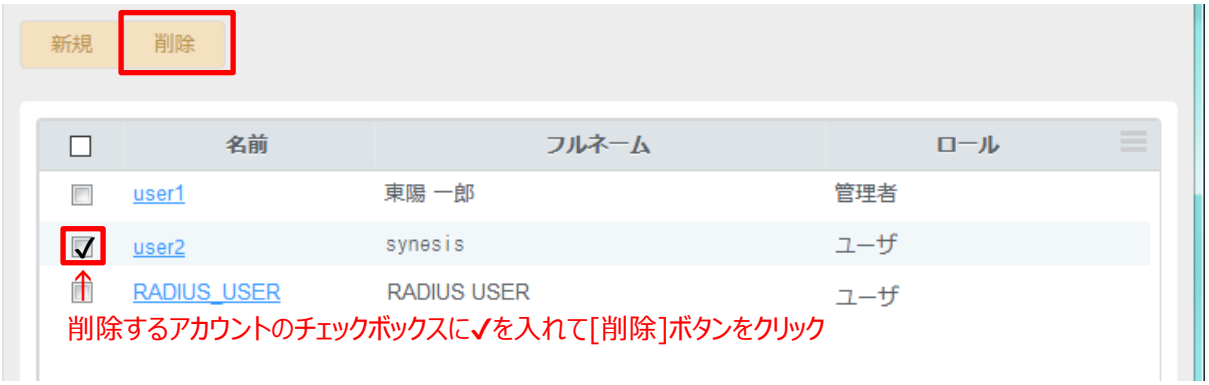
1) アカウントを新規追加する場合は、[**新規**]ボタンをクリックします。
アカウントを変更する場合は、該当するユーザ名のリンクをクリックします。



2) ユーザープロファイル画面が表示されます。必要事項を入力して、[**保存**]ボタンをクリックしてください。

5.2.1.2. SYNESIS メイン GUI のアカウント削除

1) アカウントを削除する場合は、削除したいユーザ名にチェックします。
全てのユーザを選択する場合は、ラベル欄のチェックボックスをクリックします。
2) [**削除**]ボタンをクリックします。削除確認のダイアログが表示されますので、[**はい**]をクリックします。



5.2.2. Management Console

SYNESIS のローカルから Terminal を起動するか、リモートから SSH で接続します。 ※「3.2.2 SSH」参照
アカウントに利用可能な文字数、文字列に関する制限は以下の通りです。

項目	制限
ユーザ名・パスワード 文字数	16 文字まで
ユーザ名・パスワード 文字列	アルファベット(A-Z, a-z) 数字(0-9) 特殊文字(! # % & ( ) = ~ | - ^ ¥ { } [ ] @ + * ; < > , . ? _ / ¥)

5.2.2.1. Management Console のアカウント作成・変更

1) 以下のコマンドを入力し、追加・変更するユーザとそのパスワードを指定します。

```
$ sudo su -
# htpasswd /etc/nginx/synesis/.htpasswd <username>
New Password:<password>
Re-type new password: <password>
```

2) 以下のコマンドを入力し、変更した設定を読み込みます。

```
# nginx -t
# nginx -s reload
```

5.2.2.2. Management Console のアカウント削除

1) 以下のコマンドを入力し、vi エディタにて削除するユーザが記載されている行を削除します。

```
$ sudo su -
# vi /etc/nginx/synesis/.htpasswd
```

例：ユーザ”test1”を削除する場合

```
$ sudo su -
# vi /etc/nginx/synesis/.htpasswd
example:$apr1$xfAVfaqh$XR/alY.lSI3cieO9MV6de0
test1:$apr1$qMdKa3f6$py5EU9GsUoJQGzlsX4q2a0
test2:$apr1$B5L9jXBU$kWhnws.28mxX6Ii003stc0
```

この行を削除します。その後以下を入力してエディタを終了します。
:wq

2) 以下のコマンドを入力し、変更した設定を読み込みます。

```
# nginx -t
# nginx -s reload
```

5.3. iDRAC のアカウント

iDRAC のアカウントを iDRAC の GUI から編集することができます。

アカウントに関する各制限は以下の通りです。

項目	制限
最大設定ユーザ数	15
ユーザ名文字数	16 文字 ※空白を含む
ユーザ名文字列	アルファベット(A-Z, a-z) 数字(0-9) 特殊文字(! # $ % & ( ) = - ^ | { } [ ] + * ; : < > , ? _ § I)
パスワード文字数	20 文字
パスワード文字列	アルファベット(A-Z, a-z) 数字(0-9) 特殊文字(! " # $ % & () = - | { } [ ] @ + * ; : < > , . ? _ / ¥ § I)

iDRAC のアカウント登録・編集 GUI へのアクセス方法は、以下の通りです。

1) iDRAC に管理者アカウントでログインします。 ※「3.4.1 ログイン」参照

2) [**iDRAC 設定**] >[**ユーザ**]を選択します。

3) [**ユーザ**] 画面が表示されます。[**ローカルユーザ**] 欄を開いて、登録・編集を行います。

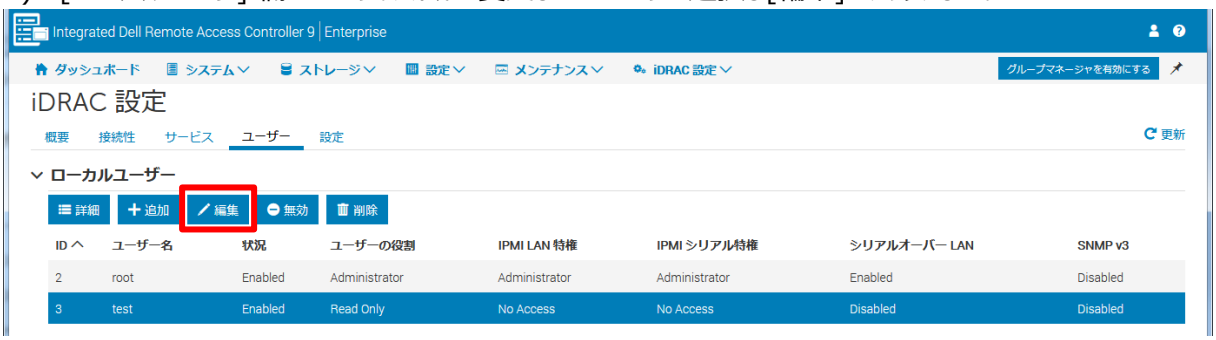
5.3.1. iDRAC のアカウント作成

1) [**ローカルユーザ**] 欄の[**追加**]ボタンをクリックします。

2) ユーザ名、パスワードを入力し、[**保存**]ボタンをクリックしてください。
必要があれば [**ユーザ特権**] 欄にて役割を指定してください。

5.3.2. iDRAC のアカウント変更

1) [**ローカルユーザ**] 欄のユーザリストから変更したいユーザを選択し[編集]をクリックします。

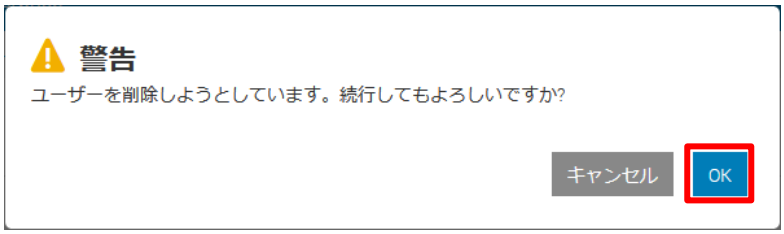


2) 設定を適宜変更し、[保存]ボタンをクリックします。

5.3.3. iDRAC のアカウント削除

1) [**ローカルユーザ**] 欄のユーザリストから削除するユーザを選択し[**削除**]をクリックします。

2) 以下のような確認のメッセージが表示されますので、[**OK**]をクリックしてください。



6. SYNESIS の監視機能

本章では、SYNESIS の監視機能を説明します。監視できる内容は、SYNESIS を構成するソフトウェアごとに異なり、それぞれ下記のようになっております。

- iDRAC：ハードウェアの異常監視（SYNESIS Portable は除く）
- SYNESIS ソフトウェア：キャプチャ動作中の異常監視、キャプチャトラフィックの状態監視

6.1. iDRAC：ハードウェアの監視

iDRAC により SYNESIS のハードウェア状態を監視できます。（SYNESIS ポータブルは除く）
また、ハードウェアに関するイベント発生時に SNMP トラップや電子メールで通知させることも可能です。

6.1.1. ハードウェア状態の確認

1) iDRAC に管理者アカウントでログインします。 ※「3.4.1 ログイン」参照
2) 以下の [**ダッシュボード**] 画面が表示されます。[**正常性情報**] 欄を確認してください。

アイコンが ⊗ になっている場合は、ハードウェアに異常が発生しています。詳細は「詳細」または、表示された項目をクリックすることで確認することができます。

6.1.2. ハードウェアイベントの通知

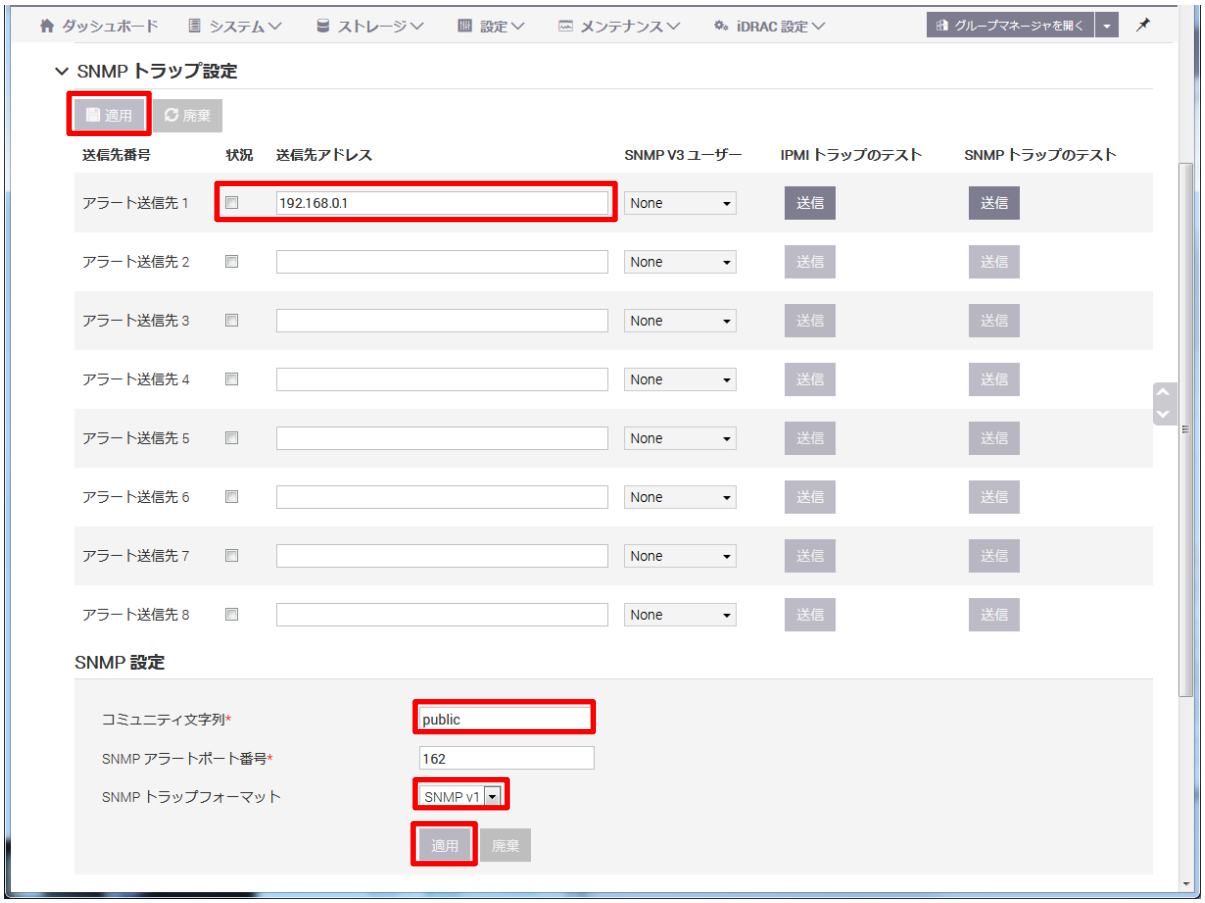
どのイベントが発生した時にどの通知先に通知するか、通知手段と通知先をイベント別に設定することができます。まず SNMP トラップやメールアドレスなどの通知手段別に通知先を登録し、その後、通知内容(イベント)と通知手段の設定を行います。

6.1.2.1. 通知先の設定

1) iDRAC に管理者アカウントでログインします。 ※「3.4.1 ログイン」参照
2) 画面上部のメニューから [**設定**] – [**システム設定**] を選択します。

[SNMP Trap で通知する場合]

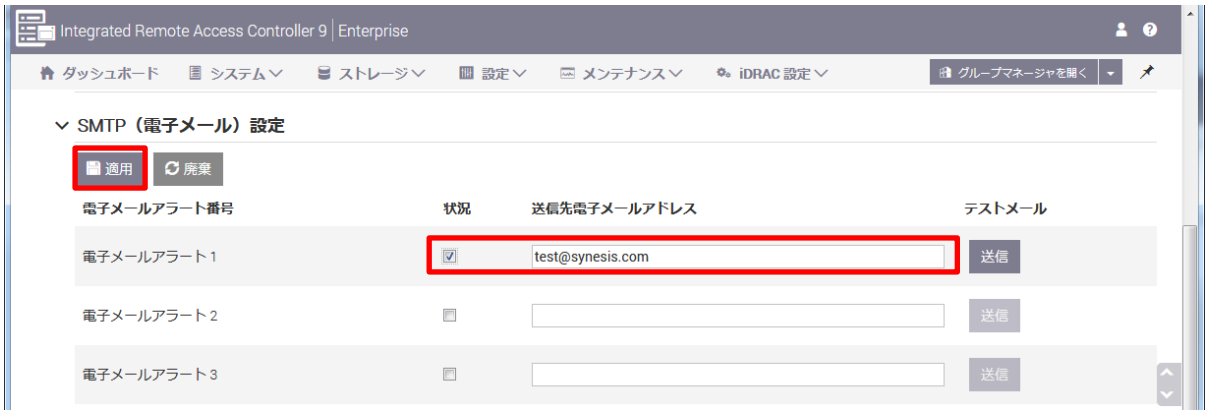
3) [**アラート設定**]>[**SNMP トラップ設定**] を開きます。
4) 「アラート送信先 1 (登録済みの場合は 2 以降で可)」を選択し、下記項目を設定します。
   - 選択した行の [**状況**] にチェックを入れる
   - [**送信先アドレス**] に SNMP マネージャー(送信先)の IP アドレスを入力
5) 設定後、[**SNMP トラップ設定**] 欄の[**適用**]ボタンをクリックします。



6) [**SNMP 設定**] 欄にて下記項目を設定し、[**適用**]ボタンをクリックします。
   - 「**コミュニティ文字列**」に任意のコミュニティ名を入力
   - 「SNMP トラップフォーマット」にてフォーマットを選択

[電子メールで通知する場合]

3) SMTP サーバの設定が済んでいることを確認します。 ※「4.3.2 SMTP サーバの設定」参照
4) [**アラート設定**] >[**SMTP(電子メール)設定**] を開きます。
5) 「電子メールアラート 1 (登録済みの場合は 2 以降で可)」の下記項目を設定します。
   - 選択した行の「**状況**」にチェック
   - 「**送信先電子メールアドレス**」に送信先メールアドレスを入力

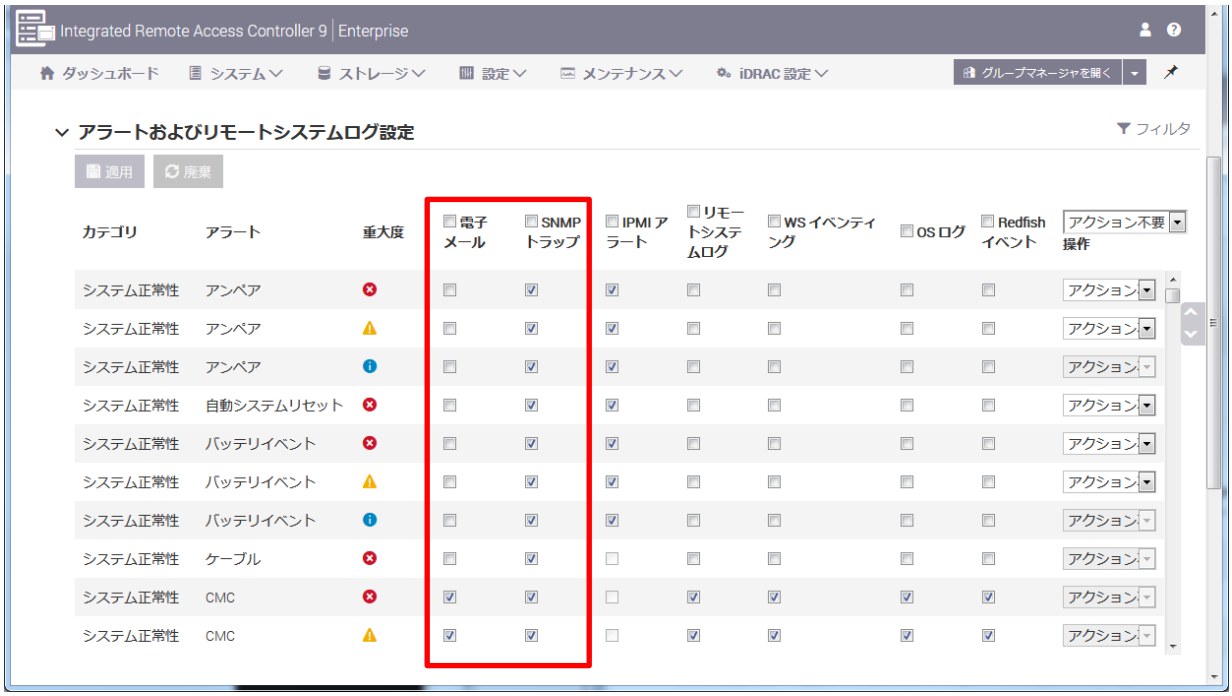


6) 設定後、[**SMTP(電子メール)設定**] 欄の[適用]ボタンをクリックします。

6.1.2.2. 通知内容・通知手段の設定

1) iDRAC に管理者アカウントでログインします。 ※「3.4.1 ログイン」参照
2) 画面上部のメニューから [**設定**] – [**システム設定**] を選択します。
3) [**アラート設定**] の [**アラート**] 欄で [**有効**] を選択し、[**適用**]ボタンをクリックします。

4) [**アラートおよびリモートシステムログ設定**] 欄を開き、発生時に通知を行いたいイベントと通知手段(SNMP Trap/電子メール)を設定します。



画面にはイベントの一覧が表示されています。通知を行いたいイベントにて、利用したい通知手段(SNMP Trap/電子メール)にチェックをして、[**適用**]ボタンをクリックします。

どのイベントを通知すべきか判断に迷う場合は、重大度が「警告」と「重要」であるイベントを通知することを推奨いたします。「警告」と「重要」のイベントを選択する場合は、以下を参照ください。

【重大度「警告」と「重要」のイベントを通知する場合】

5) [**フィルタ**]をクリックし、重大度「**情報**」のチェックを外します。

6) [**適用**]ボタンをクリックしてください。
イベント一覧に重大度が「警告」と「重要」であるイベントだけが表示されます。

7) 利用する通知手段を選択し、表示されているイベント全てをチェックします。
8) 全てのイベントに対して通知手段を設定できたら、[**適用**]ボタンをクリックします。

6.2. SYNESIS ソフトウェア：キャプチャ動作中の異常監視

SYNESIS ソフトウェアでは、キャプチャ動作中に以下の項目の状態を監視し、イベント発生時に通知を出すことができます。

監視項目	内容
自動保存	自動保存の失敗と保存先の切り替えを通知
リンクステータス	キャプチャポートのリンクステータスの変化を通知
ドロップ	キャプチャ中のドロップパケット発生を通知

SNMP トラップやメールアドレスなど、通知手段ごとに通知先を登録し、登録した通知先を通知グループに登録します。イベント発生の通知をどこに出すかは、イベントごとに通知グループで指定しできます。
通知先・通知グループの登録方法は「6.2.1 通知先、通知手段の設定」を、イベント発生の通知先(通知グループ)の指定方法は「6.2.2 通知するイベントの設定」を参照してください。

6.2.1. 通知先、通知手段の設定

SNMP トラップやメールアドレスなど、通知手段ごとに通知先を登録して、登録したそれらの通知先を通知グループに登録する手順は以下の通りです。

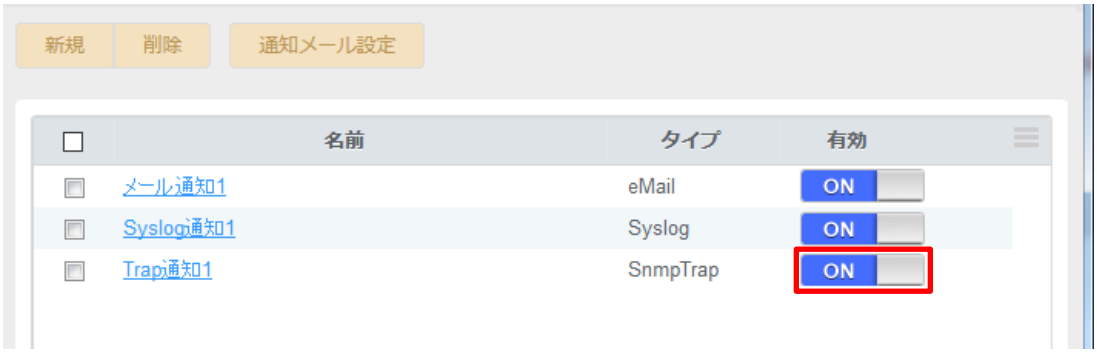
1) SYNESIS に管理者アカウントでサインインします。 ※「3.3.1.1 サインイン」参照
2) ツールバーの構成  アイコンをクリックしてください。

3) [**構成**] メニューが表示されます。[**アラートと通知**]>[**通知先**] を選択してください。

4) [**通知先**] 画面が表示されます。画面上部の[**新規**]ボタンをクリックします。

5) 通知先登録画面が表示されます。
通知手段を選択し、通知先を設定して、[**保存**]ボタンをクリックしてください。設定した通知先がリストに追加されます。

6) 設定した通知先の [**有効**] 欄が ON になっていることを確認します。

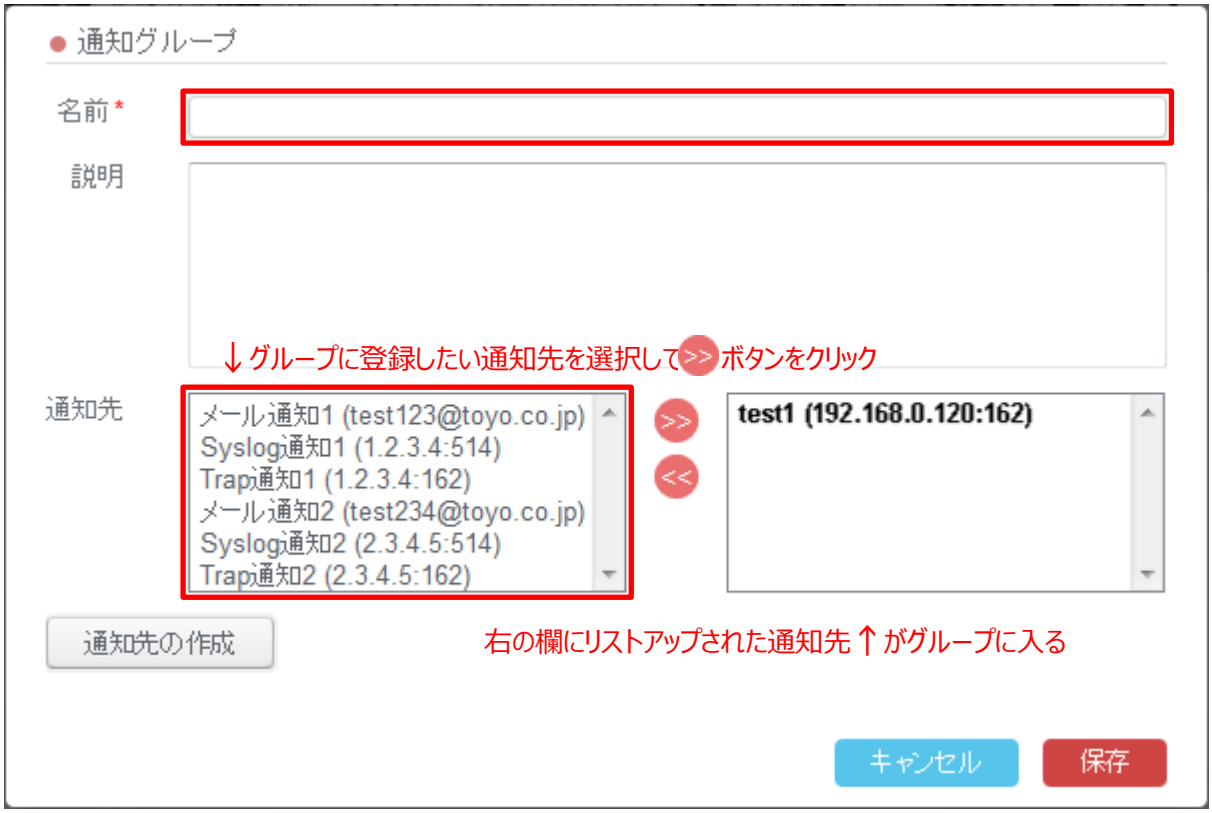


7) 続いて [**通知先**] で登録した個々の通知先を通知グループに登録します。
[**構成**]>[**アラートと通知**]>[**通知グループ**] を選択します。

8) [**通知グループ**] 画面が表示されます。画面上部にある [**新規**] ボタンをクリックします。

9) 通知グループ登録のダイアログが表示されます。以下の項目を設定します。

- 「**名前**」欄に登録したい通知グループのグループ名を入力
- 「**通知先**」欄でグループに登録したい通知先(複数可)を選択



左側の欄に登録済みの通知先が表示されます。
左側の欄から登録したい通知先を選択し、>>ボタンをクリックします。 選択した通知先が右の欄に移動します。右側の欄にリストアップされた通知先がその通知グループに登録されます。

10) 設定後、[**保存**]ボタンをクリックします。

11) 設定した通知グループが一覧に追加されます。必要に応じて[**通知テスト**]ボタンをクリックして、通知テストを実行してください。

「通知テスト」は通知の送信が実行できるかのテストになります。実際に通知が受信されたかどうかは受信側で確認ください。

6.2.2. 通知するイベントの設定

監視項目ごとに、イベントの発生が検出された際に通知を行うか否か、通知を行う場合はどの通知先(通知グループ)に通知するかを設定できます。
設定手順は以下の通りです。

1) SYNESIS に管理者アカウントでサインインします。 ※「3.3.1.1 サインイン」参照
2) 画面左端のメニューリストから [**エージェント**] を選んでクリックします。

3) [**概要**] タブの[**オプション**]ボタンをクリックします。
キャプチャオプション画面が表示されますので、[**通知設定**] タブを選択します。

4) 通知するイベントの「**有効**」にチェックし、通知先(設定済みの通知グループ)を選択した上で、[**適用**]ボタンをクリックします。

6.3. SYNESIS ソフトウェア：キャプチャトラフィックの状態監視

SYNESIS ソフトウェアでは、キャプチャしたトラフィックについて下記項目の状態を監視し、予め設定した閾値を超えた場合にアラートを発生・記録します。アラート発生時には併せて通知を出すことができます。
アラートを設定可能な項目は、以下の通りです。

カテゴリ	項目	説明
DLC	総パケット	総パケットの数で閾値を設定します。 データ対象：全チャネル合計 サンプリング周期：1 秒
	双方向 ビットレート	ビットレートで閾値を設定します。 データ対象：全チャネル合計 サンプリング周期：1 秒
ARP	ARP	解析モジュールを 1 つでも有効にした場合、自動的に解析されます。 解析された ARP パケットの数で閾値を設定します。閾値の設定は、同一送信元 MAC アドレスでの ARP の個数です。 データ対象：解析済みデータ サンプリング周期：1 分
NPM	総パケット	NPM で解析された各フローの総パケット数で閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
	双方向 ビットレート	NPM で解析された各フローのビットレートで閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
	受信パケット	NPM で解析された各フローの受信パケット数で閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
	受信 ビットレート	NPM で解析された各フローの受信ビットレートで閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
	送信パケット	NPM で解析された各フローの送信パケットで閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
	送信 ビットレート	NPM で解析された送信ビットレートで閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
APM	ART	APM で解析された各フローの ART で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分
	PTT	APM で解析された各フローの PTT で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分
	NRT	APM で解析された各フローの NRT で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分
	SRT	APM で解析された各フローの SRT で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分

	CRT	APM で解析された各フローの CRT で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分
	遅延	APM で解析された各フローの遅延で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分
	リトライ	APM で解析された各フローのリトライ A で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分

サンプリング周期は、検出間隔です。

DLC 以外のカテゴリは、解析の実施が必要です。

詳細は、SYNESIS ユーザガイドの「14. アラート機能と通知」を参照してください。

6.3.1. アラートの設定

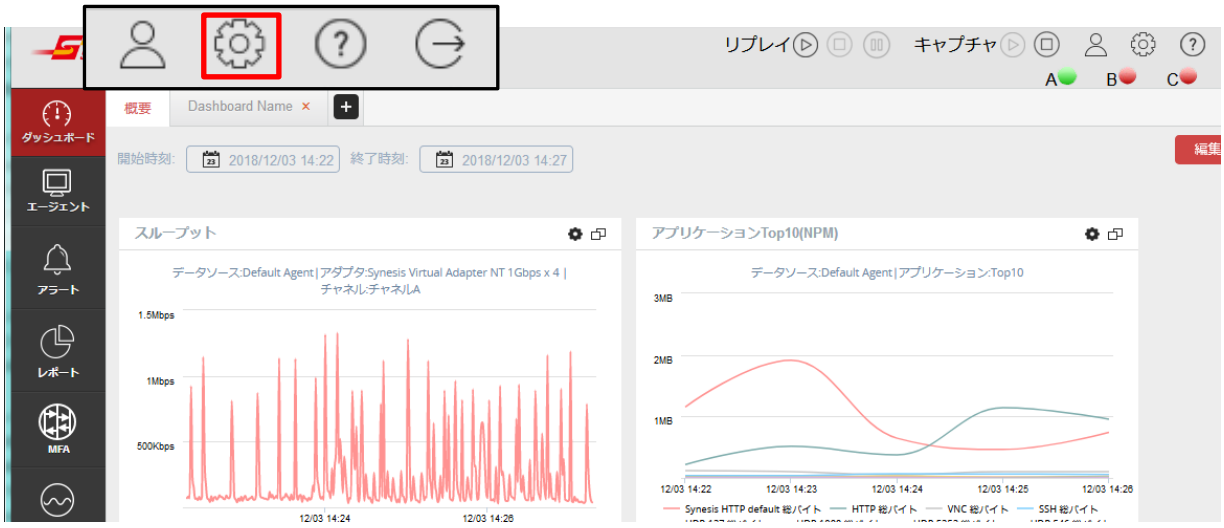
アラートを発生させるための閾値と、そのアラートが発生した場合の通知先を設定できます。

アラートの通知先はアラートごとに、登録済みの通知先から選択可能です。通知先の登録方法は「6.2.1.通知先、通知手段の設定」を参照してください。

アラートの設定方法は以下の通りです。

1) SYNESIS に管理者アカウントでサインインします。 ※「3.3.1.1 サインイン」参照

2) ツールバーの構成アイコンをクリックしてください。



3) [**構成**] メニューが表示されます。[**アラートと通知**]>[**アラート**] を選択してください。

4) アラートを発生させたい項目が属するカテゴリのタブ(DCL, ARP, NPM, APM)を選択し、[**新規**]ボタンをクリックします。

5) アラート登録画面が表示されます。閾値、通知先などを設定して、[**保存**]ボタンをクリックしてください。

6) 設定したアラームが一覧に追加されます。通知先の登録方法は「6.2.1.通知先、通知手段の設定」を参照してください。

7) 追加されたアラートの [**有効/無効**] 欄が ON になっていることを確認してください。

6.4. Management Console : SYNESIS の異常監視

Management Console の Fault Detect 機能を使用して、SYNESIS の各種異常状態を監視することができます。Fault Detect 機能は、Management Console の [Fault Detect]タブをクリックして表示される画面で設定します。

6.4.1. 監視内容

各監視項目の監視内容を以下に示します。

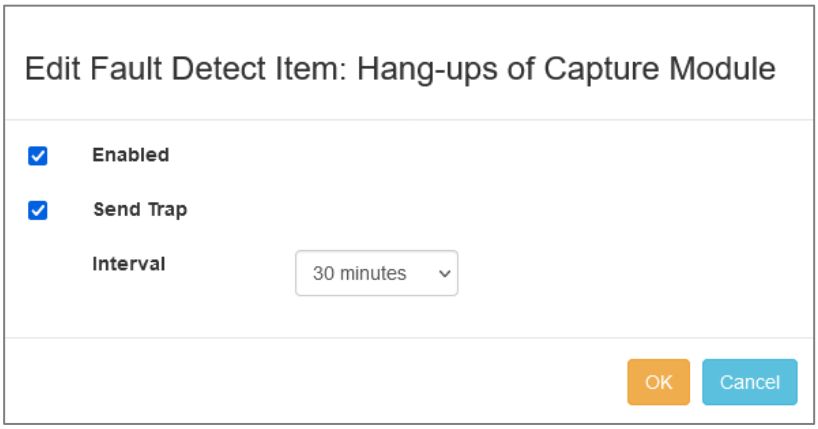
監視項目	監視内容
Hang-ups of Capture Module	パケットキャプチャ中にキャプチャ処理がハングアップしているかどうかを監視します。ハングアップを検知した場合は、パケットキャプチャのサービスを再起動します。
Capture Failures	パケットが流れているにも関わらずキャプチャできていない事象の有無を監視します。
Packet Drops	パケットキャプチャ中にパケットドロップが発生しているかどうかを監視します。
Errors in Feed Service	FeedService の通信エラーおよびデータエラーの有無を監視します。
Feed Service Restart	FeedService が再起動したかどうか、および停止状態にあるかどうかを監視します。

6.4.2. 監視項目の設定

監視項目毎に、監視の有効/無効、監視間隔、SNMP Trap による通知をするかどうか、を設定することができます。

以下に設定手順を示します。

1) 「List of Fault Detection Items」表中の[Edit]ボタンをクリックすると、以下のダイアログが表示されます。



2) 以下の項目を設定し[OK]ボタンをクリックします。

- Enabled: この項目をチェックすると監視が有効になります
- Send Trap: この項目をチェックすると、異常検知時に有効なすべての Trap サーバへ通知します
- Interval: 監視間隔を選択します

3) 監視項目を Enabled に変更した場合、「List of Fault Detection Items」表の「Status」が「Enabled」に変化します。

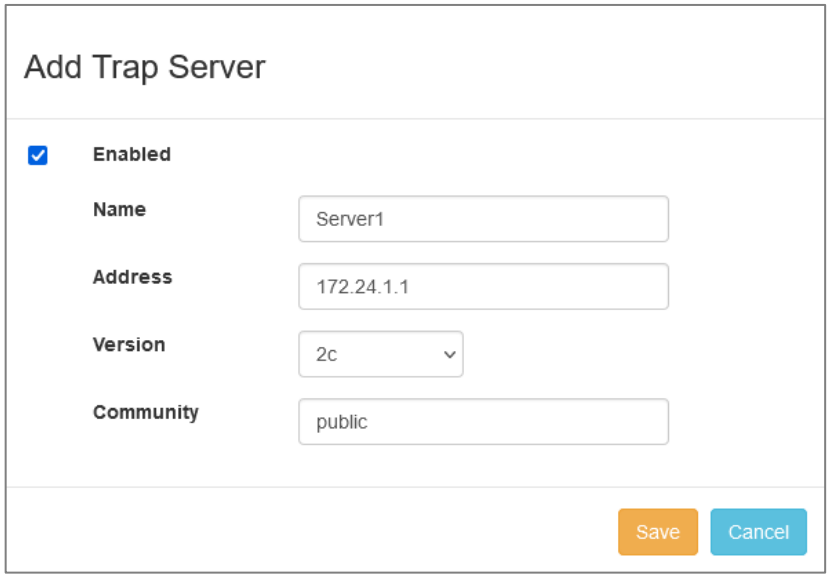
List of Fault Detection Items :

Status	Detect Item	Interval	Trap	Operation
Enabled	Hang-ups of Capture Module	30 minutes	ON	Edit Log
Disabled	Capture failures	30 minutes	OFF	Edit Log
Disabled	Packet Drops	30 minutes	OFF	Edit Log
Disabled	Errors in feed Service	10 minutes	OFF	Edit Log
Disabled	Feed Service Restart	10 minutes	OFF	Edit Log

6.4.3. Trap サーバの追加

異常検知時に通知する SNMP Trap サーバを複数追加することができます。
Trap 通知の仕様は **6.5.3 Trap 通知の仕様**を参照ください。ただし、新仕様(Revision 1)のみのサポートとなります。
以下に Trap サーバの追加手順を示します。

1) 「List of Trap Servers」表の右上にある[+Add Server]ボタンをクリックすると、以下のダイアログが表示されます。



2) 以下の項目を設定し[Save]ボタンをクリックします。

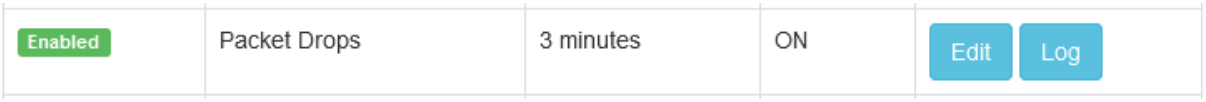
- Enabled: この項目をチェックすると当サーバへの通知が有効になります
- Name: サーバ名
- Address: サーバの IP アドレス
- Version: SNMP Version を 1 または 2c から選択します
- Community: コミュニティ名を指定します

3) 追加したサーバ情報は「List of Trap Servers」表に追加されます。

4) 追加したサーバへテスト用のトラップを送信する場合は、表中の[Test]ボタンをクリックします。

6.4.4. 監視ログの表示

「List of Fault Detection Items」表中の[Log]ボタンをクリックすると、監視ログを表示するダイアログがポップアップします。またログが存在する場合、ダイアログの「Download Full」ボタンをクリックすることで、監視ログファイルをダウンロードすることができます。



6.5. 通知の仕様

アラートの通知設定を行った場合の通知の仕様について説明します。通知は以下が対象です。

1. DLC, ARP, NPM, APM アラート設定に伴う通知
2. 自動保存イベントの通知
3. リンク状態変更イベントの通知
4. パケットドロップイベントの通知
5. マイクロバーストアラートの通知
6. 周期レポートの通知(レポートの通知先は Email のみ使用可能)

6.5.1. Email 通知の仕様

1. DLC, ARP, NPM, APM アラートの場合

- 件名: "<title>(<description>)"
  - <title>: 通知メール設定の「件名」([構成]ボタン>「通知先」>[通知先メール設定])
  - <description>: アラートで設定した「説明」([構成]ボタン>[アラート])
- 本文: "<agent name> : N/A"
  - <agent name> : エージェント名(ex. "Default Agent")
- 添付ファイル: なし

2. 自動保存イベントの場合

- 件名: "<title>(Auto Backup)"
  - <title>: 通知メール設定の「件名」([構成]ボタン>「通知先」>[通知先メール設定])
- 本文: イベント内容
  - 自動保存失敗の場合"Failed to auto backup to any directories."
  - プライマリへの切り替えの場合"Switch auto backup target directory to primary."
  - セカンダリへの切り替えの場合"Switch auto backup target directory to secondary."
- 添付ファイル: なし

3. リンク状態変更イベントの場合

- 件名: "<title>(LinkStatus Alarm)"
  - <title>: 通知メール設定の「件名」([構成]ボタン>「通知先」>[通知先メール設定])
- 本文: "<agent name> : Link Status <from>-><to> NIC:<nicid> PORT:<port>"
  - <agent name> : エージェント名(ex. "Default Agent")
  - <from>: 変化前の状態("Up" または "Down")
  - <to>: 変化後の状態("Down" または "Up")
  - <nicid>: アダプターID
  - <port>: ポート番号
- 添付ファイル: なし

4. パケットドロップイベントの場合

- 件名: "<title>(PacketDrop Alarm)"
  - <title>: 通知メール設定の「件名」([構成]ボタン>「通知先」>[通知先メール設定])
- 本文: "<agent name> : Packet Drop NIC:<nicid> PORT:<port>"
  - <agent name> : エージェント名(ex. "Default Agent")
  - <nicid>: アダプターID
  - <port>: ポート番号
- 添付ファイル: なし

5. マイクロバーストアラートの場合

- 件名: "<title>(Microburst threshold <threshold id>)"
  - <title>: 通知メール設定の「件名」([構成]ボタン>「通知先」>[通知先メール設定])
  - <threshold id>: マイクロバースト閾値設定の「閾値」番号 (1-2) ([構成]ボタン>「マイクロバースト」)
- 本文: "<agent name> : Exceeded threshold <threshold>% <count> times, maximumutilization <max-util>%, total duration <total-duration> usec"
  - <agent name> : エージェント名(ex. "Default Agent")
  - <threshold>: マイクロバースト閾値設定の「使用率」
  - <count>: この 1 分間でアラート条件を満たした回数
  - <max-util>: この 1 分間で記録した最大使用率
  - <total-duration>: この 1 分間でアラート条件を満たした合計時間
- 添付ファイル: なし

6. 周期レポート通知の場合

- 件名: "<title>(<plan-name>)"
  - <title>: 通知メール設定の「件名」([構成]ボタン>「通知先」>[通知先メール設定])
  - <plan-name>: レポートプランの「プラン名」([レポート]メニュー>[レポートプラン]タブ)
- 本文: レポートプランの「説明」([レポート]メニュー>[レポートプラン]タブ)
- 添付ファイル: レポートファイル

6.5.2. Syslog 通知の仕様

Syslog の通知フォーマットは RFC3164 の既定に従います。

- Facility: 通知先設定の「ファシリティ」 ([構成]ボタン>「通知先」)
- Severity: 通知先設定の「危険度」 ([構成]ボタン>「通知先」)
- Timestamp: 事象発生時
- Hostname: 通知先設定の「サーバ」 ([構成]ボタン>「通知先」)
- Tag: "SYNESIS Notification"
- Content:
  - DLC, ARP, NPM, APM アラートの場合: "<title>: <agent name> : N/A"
    <title>: アラート設定で指定した「説明」 ([構成]ボタン> [アラート])
    <agent name> : エージェント名(ex. "Default Agent")
  - 自動保存イベントの場合: "Auto Backup: <detail>"
    <detail>: Email 通知の「本文」と同じ
  - リンク状態変更イベントの場合: "Link Status: <detail>"
    <detail>: Email 通知の「本文」と同
  - ドロップイベントの場合: "Packet Drop: <detail>"

<detail>:Email 通知の「本文」と同じ

  - マイクロバーストアラートの場合: "Microburst threshold <threshold id>: <detail>"

<threshold id>: マイクロバースト閾値設定の「閾値」番号 (1-2) ([構成]メニュー>「マイクロバースト」)
<detail>: Email 通知の「本文」と同じ

6.5.3. Trap 通知の仕様

旧仕様と新仕様を SYNESIS の設定で切り替えることができます。
設定の詳細はユーザガイドの「14.3.1. 通知先の設定」を参照してください。

Revision 0 (旧仕様)

- Trap OID: 1.3.6.1.4.1.36875(全 Trap で共通)
- パラメータ
  - Description
    - OID: 1.3.6.1.4.1.36875.1
    - Type: 文字列
    - 値: Syslog 通知の「Content」と同じ

Revision 1 (新仕様)

- Trap OID: 1.3.6.1.4.1.36875.2.5.0.x (Trap 種別毎に末尾の ID が異なります)
- パラメータの OID や内容の詳細は MIB ファイル(TOYO-SYNESIS-MIB.mib)を参照ください

7. Portable モデルのディスク情報

7.1. 故障の検知

Distributed モデルでは iDRAC でディスク故障を検知できますが、Portable モデルではその手段がないため、SYNESIS の機能としてその手段を提供します。
具体的には、ユーザが SYNESIS にサインインしたタイミングで、何らかの故障・障害がある場合には、ダイアログでその内容を通知します。また、コンソールでコマンドを入力することにより、手動で故障の有無を確認することもできます。

7.1.1. 対象ベースユニット

本機能が有効なベースユニットは、SYNESIS 文書一覧から「諸元一覧」を開き、「4. Control Unit の仕様一覧」で確認してください。

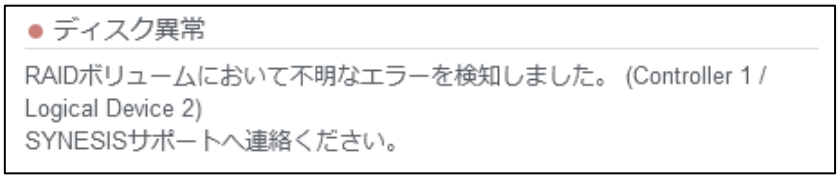
7.1.2. サインイン時の故障通知内容

以下の故障がある場合にメッセージが表示されます。

7.1.2.1. 論理デバイス異常

本メッセージが表示された場合は、サポートに問い合わせください。

7.1.2.2. 論理デバイス異常・不明なエラーがある場合のメッセージ



本メッセージが表示された場合は、サポートに問い合わせください。

7.1.2.3. 物理デバイス異常・スロット抜けがある場合のメッセージ

本メッセージが表示された場合は、サポートに問い合わせください。

7.1.2.4. 物理デバイス異常・リビルド中がある場合のメッセージ

本メッセージが表示された場合は、RAID の再構築が完了するまで電源を入れたまま待機する必要があります。
RAID の再構築が完了したかどうかは、コマンドによる故障検知にて確認が可能です。

7.1.2.5. 物理デバイス異常・ディスク故障がある場合のメッセージ

本メッセージが表示された場合は、サポートに問い合わせください。

7.1.3. コマンドによる故障検知

手動でディスク故障を確認する場合は、下記のコマンドを実行します。

```
$ sudo /usr/local/synesis/synesis_tools/SSDchecker/diskFailureChecker [-h]
```

-h オプションでヘルプを表示します。

故障がない場合は、以下の通り OK と表示されます。

```
$ sudo /usr/local/synesis/synesis_tools/SSDchecker/diskFailureChecker
OK
```

故障がある場合は、以下のように論理デバイス番号、物理デバイス番号、故障の内容が表示されます。

```
$ sudo /usr/local/synesis/synesis_tools/SSDchecker/diskFailureChecker
Controller 1 / Logical Device 1 / PHY 2 : Rebuilding
```

7.1.4. ログイン時の故障検知無効化

故障検知機能はディスクアクセスが発生するため、キャプチャおよびリプレイの性能に影響があります。ログイン時の故障検知を無効化して、性能を優先したい場合は、以下の手順で無効化します。

1) 管理者権限で、vi 等のエディタを使い下記のファイルを開きます。

```
$ sudo vi /var/lib/tomcat/webapps/ROOT/WEB-INF/classes/common.properties
```

2) 下記のパラメータを true から false に変更します。

```
system.signin.check.diskFailure = true
```

3) ファイルを上書き保存してエディタを閉じます。

4) **2.4. SYNESIS サービスの再起動** を参考に、Tomcat サービスを再起動します。

次回ログインから故障検知が無効化されます。

7.2. SMART 情報の表示

ポータブルモデルで使用されている SSD の状態を知る手段として、ディスクの SMART 情報を Management Console で確認できます。

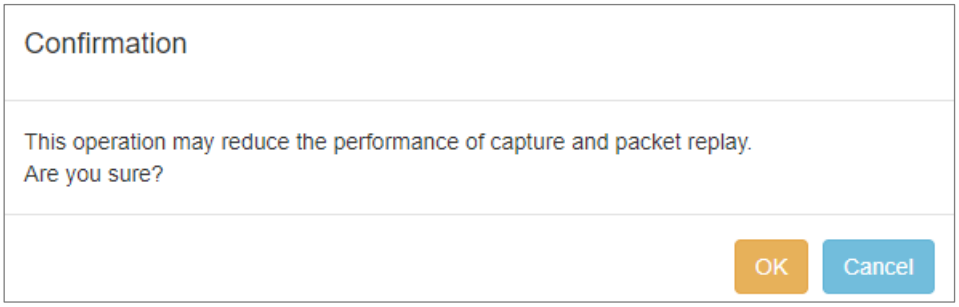
7.2.1. 対象モデル

すべてのポータブルモデルが対象です。

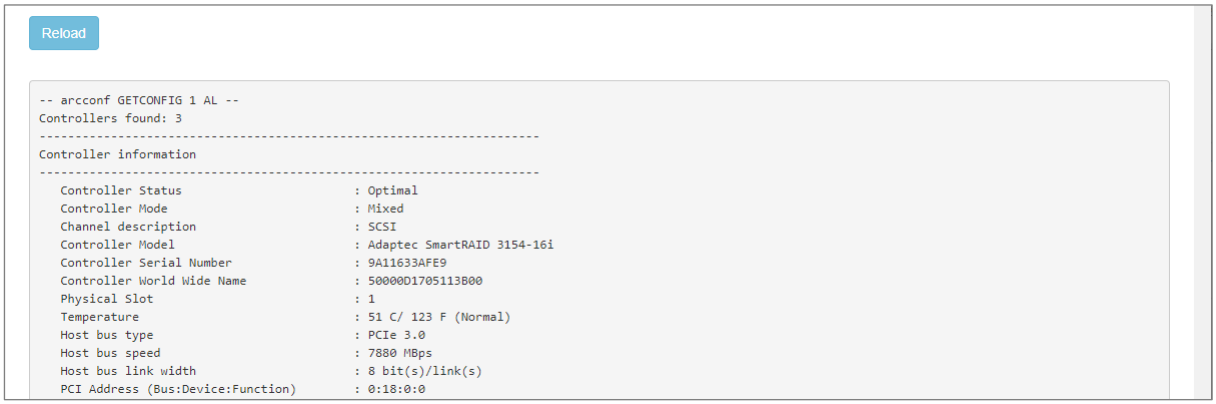
7.2.2. 操作方法

1) Management Console の [SMART]タブをクリックして、SMART 情報表示画面に移動します。初期状態では [Reload]ボタンのみ表示されています。

2) [Reload]をクリックすると下記ダイアログが表示され、キャプチャとリプレイの性能に影響があることを警告します。



3) [OK]をクリックすると、SMART 情報を取得して表示します。



7.2.3. 注意事項

SMART 情報取得の際にディスクアクセスが発生するため、キャプチャおよびリプレイの性能に影響があります。

8. 設定情報やデータのバックアップ

SYNESIS の設定やデータのバックアップを取り、故障回復後やリカバリ後に設定やデータを復元(リストア)することが可能です。
バックアップ可能なのは OS の設定情報や SYNESIS の設定情報、トレースファイル、作成されたレポートです。キャプチャデータは直接バックアップを取ることができません。キャプチャデータをトレースファイルに保存し直してバックアップを行います。
バックアップ方法はそれぞれのリンク先を、復元(リストア)方法の詳細は 8. 設定情報やデータのリストアを参照してください。

8.1. OS 設定情報のバックアップ

OS の設定内容については、OS がインストールされているディスク(デバイスファイル)を、バックアップツールなどを利用して丸ごとバックアップします。
OS がインストールされているディスク(デバイスファイル名：/dev/sda, /dev/sdb など)は、df コマンド等で確認することができます。
バックアップ作成手順は以下の通りです。

1) SYNESIS へ SSH で接続します。 ※「3.2.2 SSH」参照
2) 以下のコマンドで、OS がインストールされているディスク(デバイスファイル名)を確認します。

```
$df
Filesystem       1K-blocks       Used  Available Use% Mounted on
tmpfs              6586096     108944    6477152   2% /run
/dev/sdb2       1547582492   62045644 1406903692   5% /
tmpfs             32930468        256   32930212   1% /dev/shm
tmpfs
tmpfs
/dev/sdb1
/dev/sda       10064238080 9971579076   92659004 100% /pvc/data/packetdb1
/dev/sdc        1826388224   68439320 1757948904   4% /pvc/data/databank
tmpfs              6586096         36    6586060   1% /run/user/100
```

「/」へマウントされているデバイスファイル名(数値を除く)を確認します。
本例の場合：/dev/sdb

3) 手順 2)で確認した、OS がインストールされているディスクからシステムイメージを作成するなどして、丸ごとバックアップしてください。

8.2. SYNESIS 環境・設定情報

SYNESIS の設定情報としてライセンスファイルと 構成(コンフィグ)情報のコンフィグファイルの バックアップファイルを作成することが可能です。

8.2.1. ライセンスファイルのバックアップ

ライセンスファイルのバックアップ手順は以下の通りです。

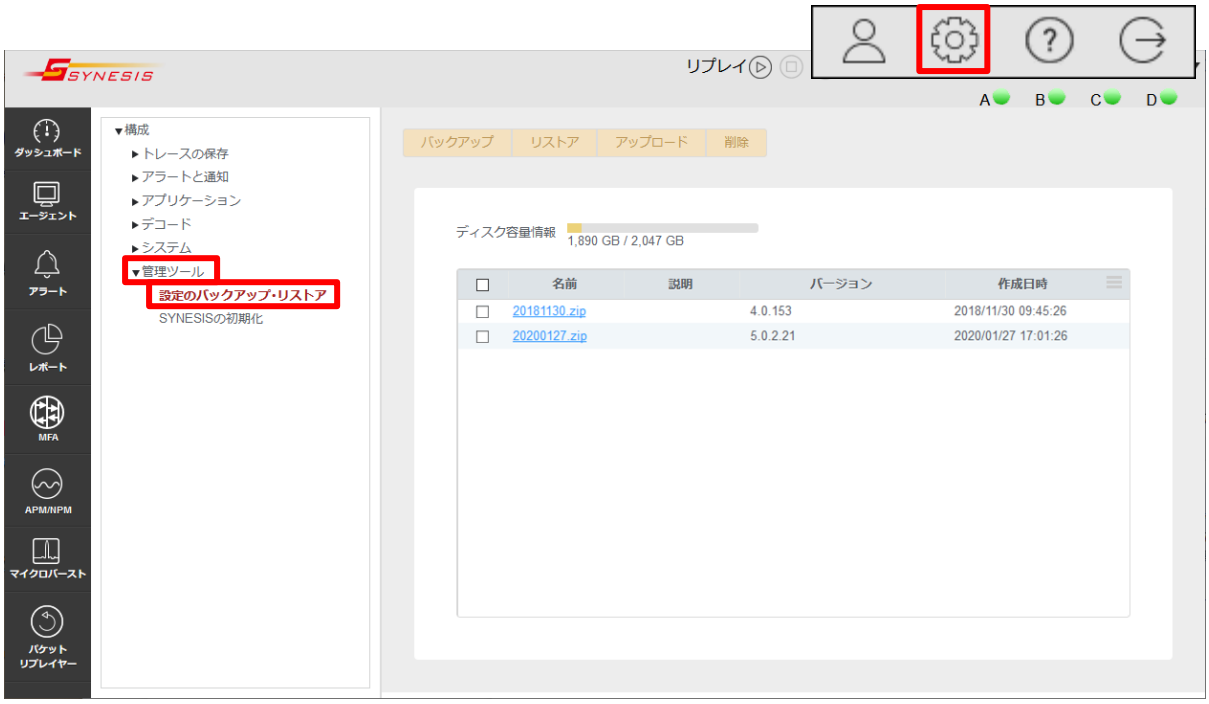
1) SYNESIS へ SSH で接続します。 ※「3.2.2 SSH」参照
2) SCP などを利用して、以下の場所にあるライセンスファイルを SYNESIS 外の外部ストレージなどにバックアップ(保存)してください。
   Path：/var/lib/tomcat/pvclicense.lic

8.2.2. コンフィグファイルのバックアップ

SYNESIS の構成（コンフィグ）情報のバックアップファイルを作成することができます。
保存される項目など、詳細はユーザガイドの「17.1 設定のバックアップとリストア」を参照してください。
コンフィグファイルのバックアップ作成手順は、以下の通りです。

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照

2) トップ画面の右側上部にある構成アイコン をクリックします。



3) [**構成**] メニュー画面が表示されます。
左側のメニューから [**管理ツール**] >[**設定のバックアップ・リストア**] を選択してください。

3) [**バックアップ**]ボタンをクリックしてください。

4) [**バックアップ**] 画面が表示されます。ファイル名を指定します。

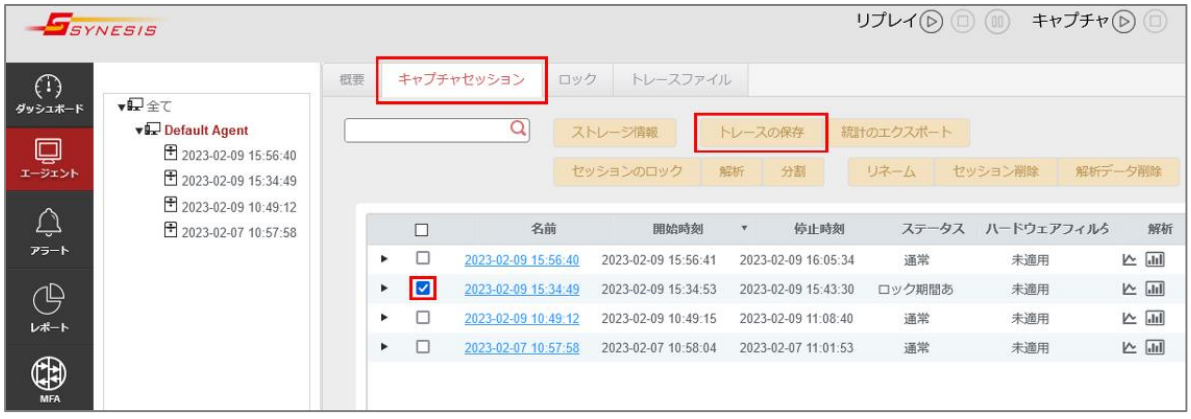
5) 入力後、[**適用**]ボタンをクリックします。
設定情報が収められたバックアップファイルが作成され、リストに追加されます。

6) 追加されたバックアップファイルの [**名前**] 欄のリンク部分をクリックしてください。
[**バックアップファイルの編集・ダウンロード**] 画面が表示され、バックアップファイルをダウンロードすることができます。

8.3. キャプチャデータのバックアップ

キャプチャしたデータは直接バックアップすることができません。
キャプチャデータをバックアップする場合は、キャプチャデータをトレースファイルに保存した状態でバックアップを行ってください。
なお、キャプチャデータがパケットストレージ領域の容量を超えた場合、キャプチャデータは古いものから順に上書きされます。上書きされたデータは、トレースファイルにすることはできませんのでご注意ください。
キャプチャデータをトレースファイルに保存する手順は、以下の通りです。

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照
2) 左側のメニューから [**エージェント**] を選択し、[**キャプチャセッション**] タブを選択します
3) トレースファイル化したいキャプチャデータを含むキャプチャセッションの左端のチェック欄にチェックを入れ、[**トレースの保存**]ボタンをクリックします。

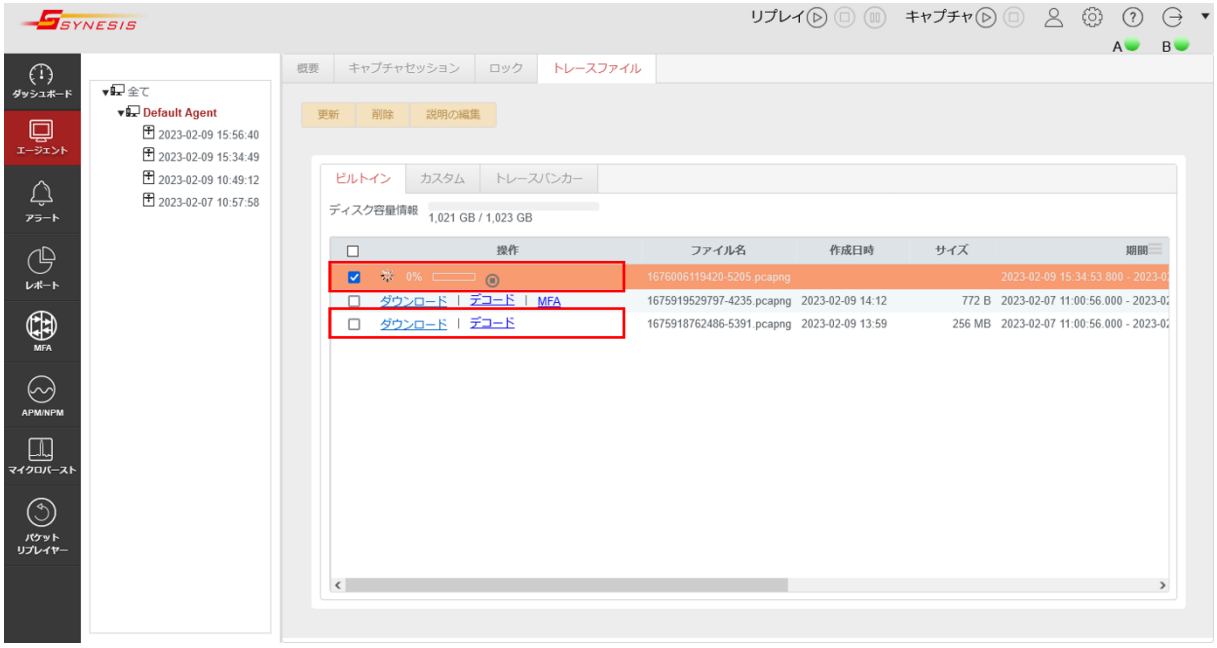


4) 期間を指定します。
期間の指定方法の詳細は、ユーザガイドの「5.トレースの保存操作」を参照してください。

5) 「**最大ファイル数**」欄に「0」と入力します。保存ファイル数の上限がなくなり、指定した期間内のデータが全て対象となります。

6) 設定画面右下の[**トレースの保存**]ボタンをクリックします。

7) 自動的に [**トレースファイル**] タブが選択された状態に切り替わります。
「**操作**」欄が「**ロード中…**」や進捗状態表示 から「**ダウンロード/デコード**」に変わったら、トレースファイル化は完了です。

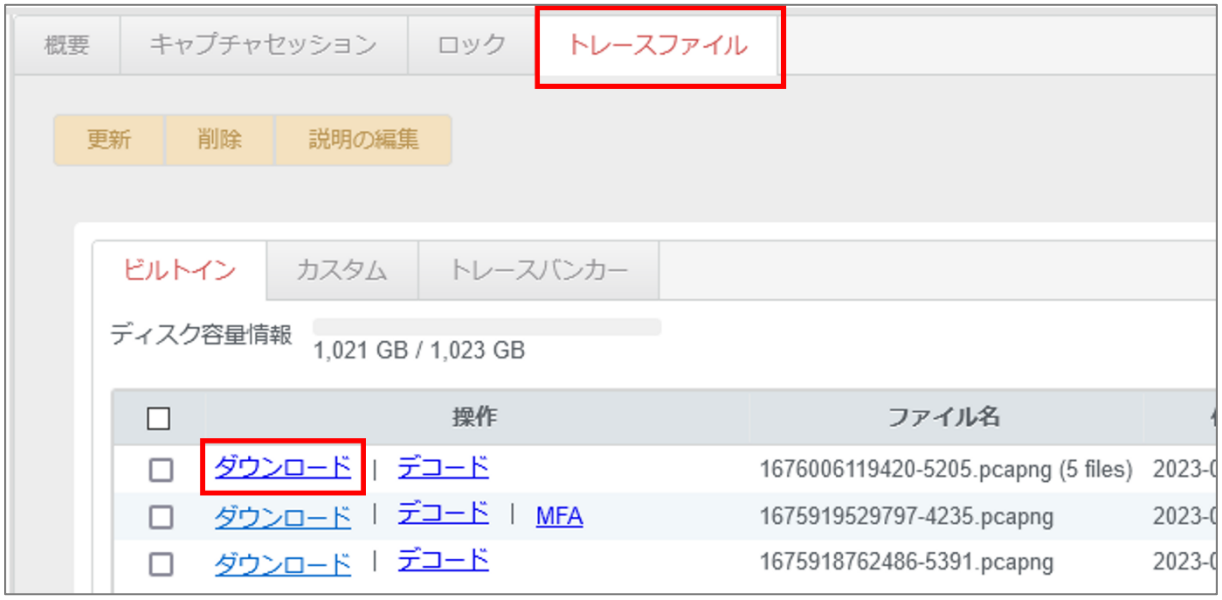


8) [**ダウンロード**] をクリックすると、トレースファイルをダウンロードし、 バックアップとして保存することができます。
バックアップしたトレースファイルのリストア方法は「9.3.トレースファイルのリストア」を参照してください。

8.4. トレースファイルのバックアップ

トレースファイルのバックアップ手順は以下の通りです。

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照
2) 左側のメインメニューから [**エージェント**] を選択し、[**トレースファイル**] タブを選択します。SYNESIS 内に保存されているトレースファイルの一覧が表示されます。
3) [**操作**] 欄の [**ダウンロード可**] をクリックして、トレースファイルをダウンロードします。



4) ダウンロードされたトレースファイルをバックアップしておきます。

8.5. 作成されたレポートのバックアップ

レポートメニューで作成されたレポートをバックアップ(保存)することが可能です。

レポートの作成に利用されるレポートテンプレートやレポートプランはコンフィグファイルのバックアップ項目に含まれます。コンフィグファイルのバックアップ手順は「**8.2.2. コンフィグファイルのバックアップ**」を参照してください。

作成されたレポートのバックアップ手順は以下の通りです。

1) SYNESIS へ SSH で接続します。 ※「**3.2.2. SSH**」参照
2) SCP などを利用して、以下のパスにあるレポートを外部ストレージなどにバックアップ(保存)してください。
   Path:/pvc/data/databank/generated_report

9. 設定情報やデータのリストア

リカバリ前に作成したバックアップファイルを使って、リカバリ後に SYNESIS の設定やデータを復元(リストア)することが可能です。
バックアップを使ってリストアできるのは OS の設定情報や SYNESIS の環境・設定情報、トレースファイルです。
それぞれの作業手順の詳細は、リンク先を参照してください。
SYNESIS のリカバリ方法については「SYNESIS リカバリ手順書」を参照してください。

9.1. OS 設定情報のリストア

8.1 OS 設定情報のバックアップの手順に従って作成されたシステムイメージを、OS がインストールされているディスク(デバイスファイル名：/dev/sda, /dev/sdb など)にリストアします。OS がインストールされているディスクは df コマンド等で確認します。
手順は以下の通りです。

1) SYNESIS へ SSH で接続します。 ※「3.2.2 SSH」参照
2) 以下のコマンドで、OS がインストールされているディスク(デバイスファイル名)を確認します。

```
$ df
Filesystem       1K-blocks       Used  Available Use% Mounted on
tmpfs              6586096     108944    6477152   2% /run
/dev/sdb2       1547582492   62045644 1406903692   5% /
tmpfs             32930468        256   32930212   1% /dev/shm
tmpfs
tmpfs
/dev/sdb1
/dev/sda       10064238080 9971579076   92659004 100% /pvc/data/packetdb1
/dev/sdc        1826388224   68439320 1757948904   4% /pvc/data/databank
tmpfs              6586096          36    6586060   1% /run/user/1000
```

「/」へマウントされているデバイスファイル名(数値を除く)を確認します。
本例の場合：/dev/sdb

3) 2）で確認できたディスクにシステムイメージをリストアします。

9.2. SYNESIS 環境・設定情報のリストア

リカバリ前、バックアップを取ったライセンスファイルやコンフィグファイルを使って、SYNESIS を元の設定に戻すことが可能です。

9.2.1. ライセンスファイルのリストア

「SYNESIS リカバリ手順書」の手順に従ってリカバリを実施し、ライセンスファイルのリストアが完了している場合は本手順の実施は不要です。
「**9.2.2. コンフィグファイルのリストア**」の手順を実行してください。

1) リモート操作の場合は下記のアドレスを Web ブラウザのアドレスバーに入力してください。
   https://<*SYNESIS IP Address*>/
2) サインイン画面が表示された場合は、本手順の実行は不要です。

そのままサインインし、「**コンフィグファイルのリストア**」を実行してください。
下図のような「デバイス ID」が表示された場合は、手順 3)を実行してください。

3) SYNESIS へ SSH で接続します。 ※「3.3.2. SSH」参照
4) SCP などを利用して、保存したライセンスファイル(pvclicense.lic)を SYNESIS のホームディレクトリへ転送します。
5) 以下のコマンド例を参考に、手順 4)で転送したファイルが保存されているディレクトリへ移動します。
デフォルトでは以下がホームディレクトリのパスです。

```
$ cd /home/synesis/
```

6) 以下のコマンドを入力し、所定の場所へライセンスファイルを移動します。

```
$ mv pvclicense.lic /var/lib/tomcat/
```

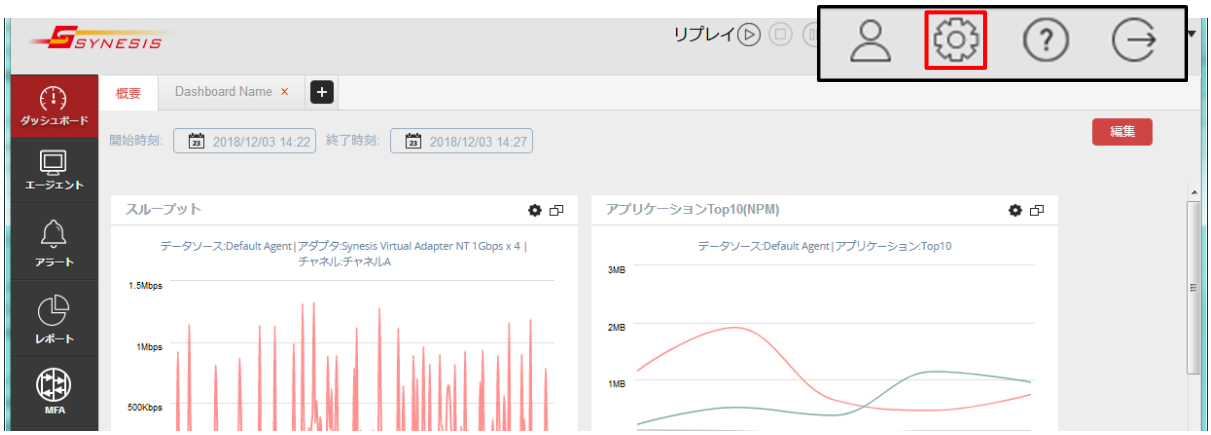
7) ブラウザで下記の URL へアクセスします。
https://<*SYNESIS IP Address*>/mgmt/
8) ユーザ名とパスワードを入力します。
ユーザ名(デフォルト) :admin
パスワード(デフォルト) :synesis1
9) 以下の画面が表示されますので、Service **[Tomcat]**の行の**[Restart]**をクリックします。

10) ブラウザで下記の URL にアクセスし、サインイン画面が表示されることを確認します。
https://<*SYNESIS IP Address*>/mgmt/

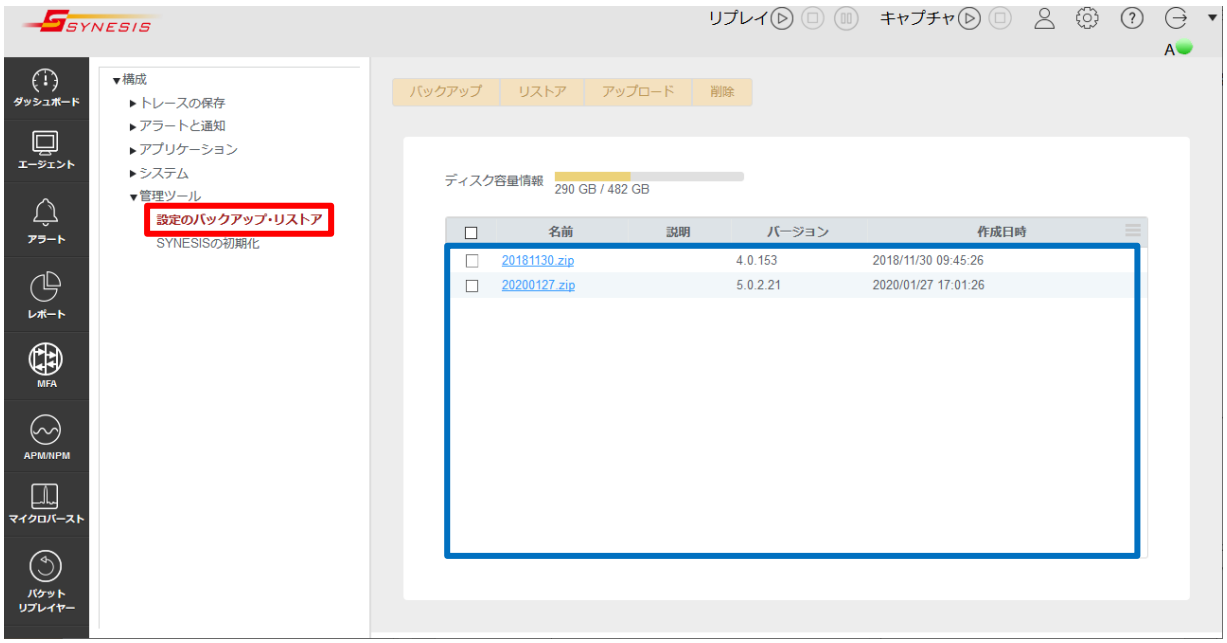
9.2.2. コンフィグファイルのリストア

「8.2.2 コンフィグファイルのバックアップ」の手順に従って作成されたバックアップを使って、SYNESIS を元の設定に戻すことが可能です。
バックアップで保存される項目についてはユーザガイドを参照してください。

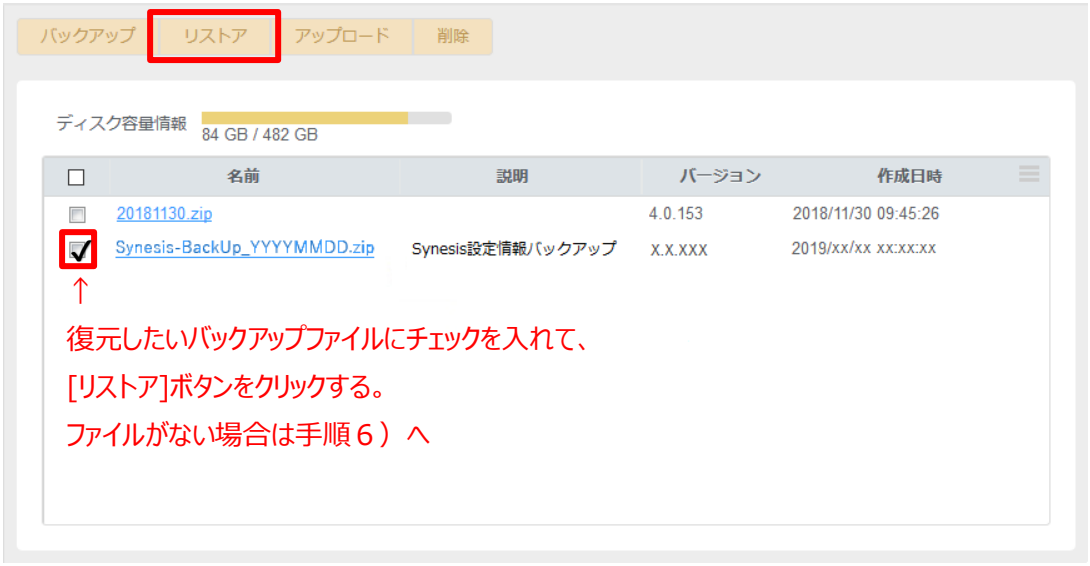
1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照
2) トップ画面の右側上部にある構成アイコンをクリックします。



3) [**構成**]メニュー画面が表示されます。左側のリストから **[管理ツール]** > **[設定のバックアップ・リストア]** を選択します。



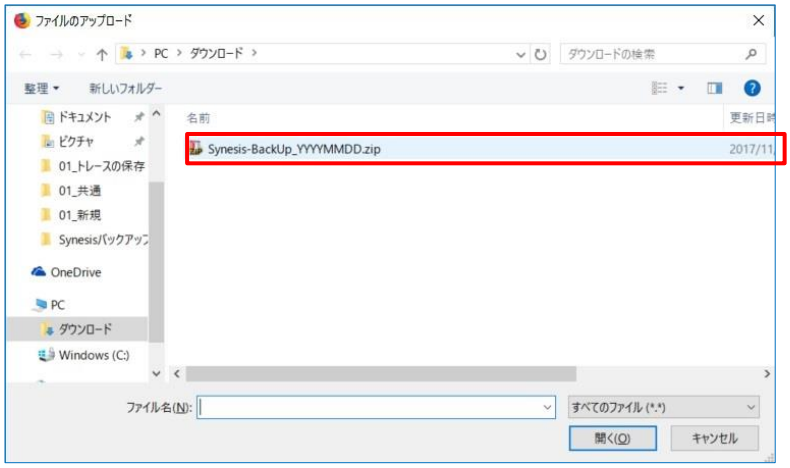
4) [**設定のバックアップ・リストア**] 画面が表示されたら、復元（リストア）するバックアップファイルが一覧(上図青枠)内にあるか確認してください。
5) リストア対象となるバックアップファイルがある場合は、ファイル名の左側にあるチェックボックスにチェックを入れて[**リストア**]ボタンをクリックし、手順 10) へ進んでください。
リストア対象となるバックアップファイルが一覧にない場合は、手順 6)に進んでください。



6) [**設定のバックアップ・リストア**] 画面の上部の**[アップロード]**ボタンをクリックしてください。

7) 以下の画面が表示されるので、**[参照]**ボタンをクリックしてください。

8) **[ファイルのアップロード]** 画面よりアップロードするファイルを選択してください。

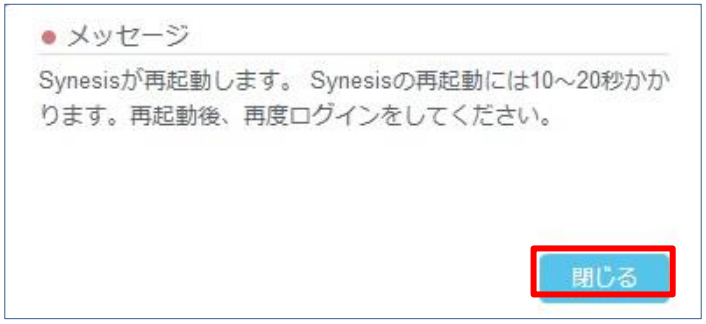


9) アップロードするファイルを選択して**[開く]**ボタンをクリックすると、[アップロード] 画面にバックアップファイルの情報が表示されます。情報を確認し問題なければ[**アップロード**]ボタンをクリックしてください。

10) アップロードしたファイルがリストに追加されていることを確認してください。ファイル名左側のチェックボックスに地チェックを入れ、[リストア]ボタンをクリックします。

11) 以下の確認画面が表示されます。 [**適用**]ボタンをクリックします。

12) リストア完了後、以下のポップアップ画面が表示されますので、確認後[**閉じる**]ボタンをクリックします。



13) SYNESIS へ再度アクセスし、サインインします。

14) 構成 アイコン をクリックし、コンフィグ(設定)情報が反映されていることを確認してください。

9.3. トレースファイルのリストア

バックアップされたトレースファイルは、SYNESIS の「トレースバンカー」機能で読み込めます。

トレースファイルを SYNESIS 外部の保存先から読み込む手順は以下の通りです。

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照

2) メインメニューから[**エージェント**] を選択し、[**トレースバンカー**]タブをクリックしてください。外部からトレースファイルを読み込ませることが可能な [**トレースバンカー**] 画面が表示されます。

3) **[アップロード]**ボタンをクリックしてください。
以下の**[アップロード]**ダイアログが表示されます。

4) **[参照]**ボタンをクリックし、読み込むファイルを指定してください。

5) [**トレースファイルをアップロード**]ボタンをクリックしてください。
指定したファイルがアップロードされ、一覧に追加されます。

9.4. レポート設定のリストア

レポートの作成に利用されるレポートテンプレートやレポートプランは コンフィグファイルのバックアップ項目に含まれており、コンフィグ情報のバックアップを使って、同じ形式のレポートを作成することが可能です。
詳細はユーザガイドの「12. レポート」を参照してください。
バックアップとして保存した作成済のレポートは、SYNESIS GUI 上では参照できません。ファイルを直接開いて参照してください。

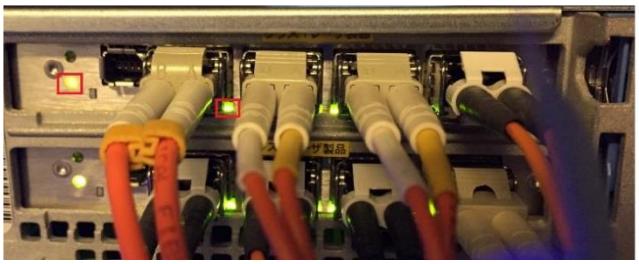
10. 簡易動作確認手順

本章では、SYNESIS の電源投入後の動作確認として実行できる、簡易動作確認手順について説明します。
障害・異常発生時の問題個所確認としてもご利用いただけます。

10.1. キャプチャポートのリンクステータス確認

スイッチやタップなど、トラフィックをキャプチャしたい SYNESIS の対向側のポートと、SYNESIS のキャプチャポートがリンクしているかどうか、リンクステータスを確認します。SYNESIS のキャプチャポートと対向側のポートを接続した上で、以下の項目を確認してください。

① 対向側のポートがトラフィックを流す設定・構成になっていること
② 対向側のポートと、SYNESIS のキャプチャポート※が接続されていること
③ 項目②で確認した SYNESIS キャプチャポートのリンク LED が「**点滅**」していること

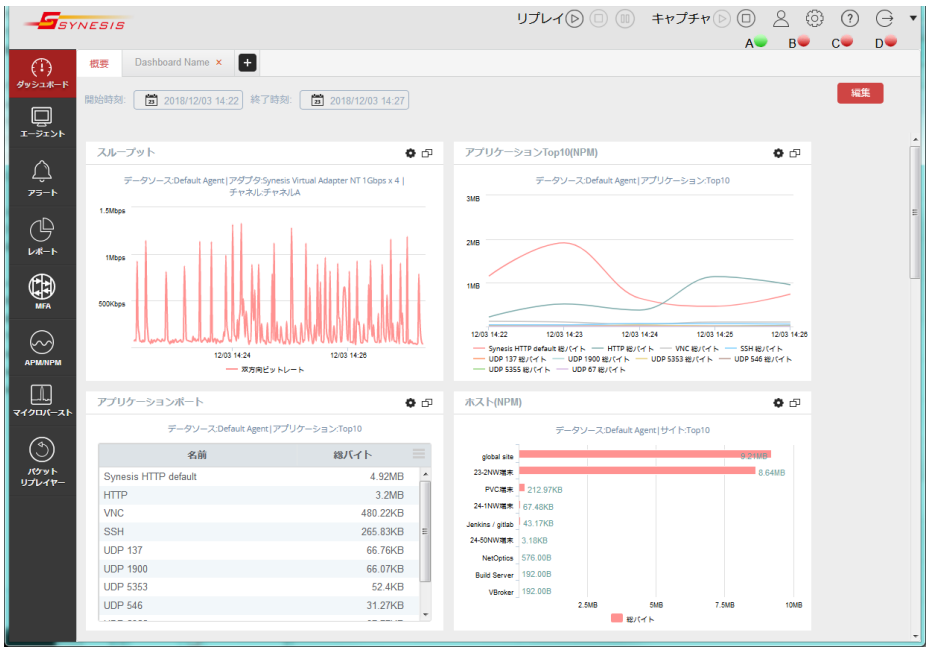


「消灯」の場合、SYNESIS の対向とリンクしていません。
「点灯」の場合、SYNESIS の対向とリンクしていますが、トラフィックが流れてきていません。
※SYNESIS のポートの位置は**[構成]** > **[SYNESIS について]**よりご確認いただけます。

10.2. SYNESIS へのアクセス

SYNESIS の電源を投入したら、正常に SYNESIS にアクセスできるかを確認してください。手順は以下の通りです。

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照
2) サインイン後、SYNESIS の [**ダッシュボード**] 画面が表示されることをご確認ください。



10.3. キャプチャの動作確認

起動した SYNESIS にアクセスできましたら、 SYNESIS の設定を確認した上でキャプチャを開始し、キャプチャが正常に行われることを確認してください。

10.3.1. SYNESIS の設定の確認

キャプチャを開始する前に、SYNESIS の設定を確認してください。確認の手順は以下の通りです。

1) ツールバー上のリンクステータスの表示が [●] になっていることを確認してください。

2) 画面左側のメニューから [**エージェント**] を選択し、[**概要**] タブ内の [**オプション**] ボタンをクリックします。

3) [**キャプチャオプション**] 画面の [**共通**] タブを表示させ、[**キャプチャ中の自動解析**] にチェックがないことを確認します。

※チェックがあった場合、チェックを外してください。

4) [**適用**]ボタンをクリックしてください。（すでにキャプチャ中の場合は、[適用]ボタンは無効になっています。）

10.3.2. キャプチャの開始

1) 画面左側のメニューから [**エージェント**] を選択してください。
2) キャプチャのステータスが ”停止” の場合は、[**キャプチャの開始**]ボタンをクリックします。
   キャプチャのステータスが “キャプチャ” の場合は、そのまま次の手順に移ってください。

3) キャプチャのステータスが “キャプチャ” に変わることを確認してください。

10.3.3. キャプチャ開始後の確認項目

キャプチャを開始後、1 ～2 分待ってから、画面内の以下項目を確認してください。

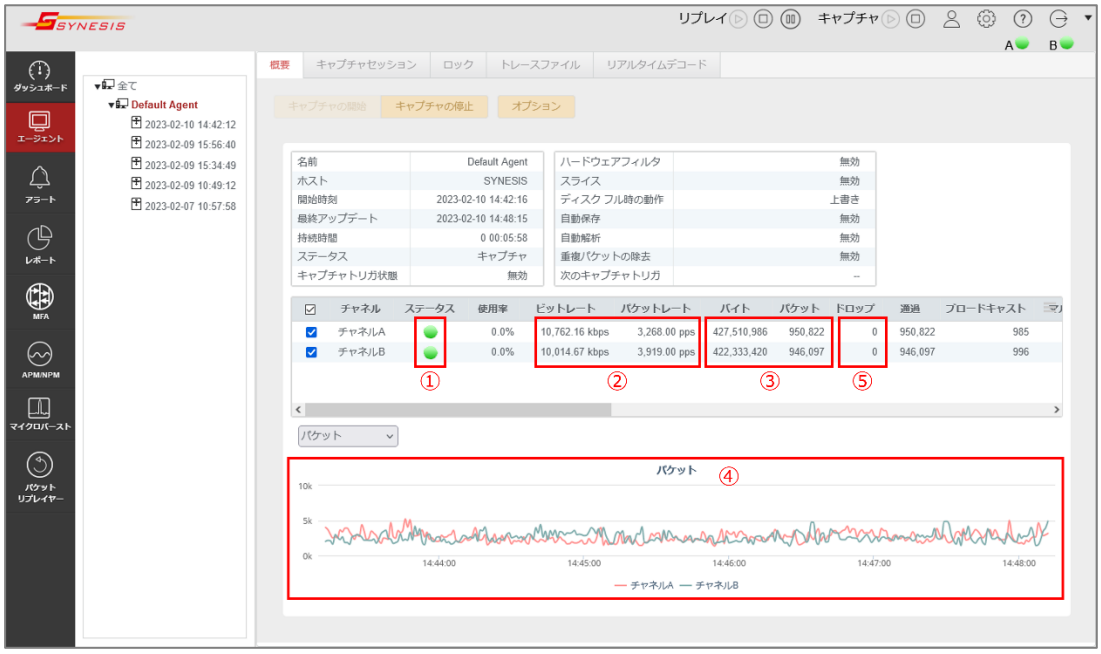
① トラフィックが流れているポート(チャネル)のステータスが “緑●” になっていること

② トラフィックが流れているポート(チャネル)の”ビットレート”、”パケットレート” に ”0(ゼロ)” 以外の数値が表示されていること

③ トラフィックが流れているポート(チャネル)の ”パケット”と”バイト”のカウントが増加すること

④ キャプチャを開始後、データがグラフにプロットされていること

⑤ “ドロップ” が ”0(ゼロ)” であること



10.4. iDRAC のステータス確認

iDRAC により、SYNESIS のハードウェアのステータスを確認することができます。

1) iDRAC にログインします。 ※「3.4.1 ログイン」参照

2) 以下のダッシュボード画面が表示されます。
画面左上の [**正常性情報**] の欄のチェックがすべて緑色であることを確認してください。

以上で簡易動作確認は完了です。ブラウザを閉じて構いません。

11.ログの種類と取得方法

11.1.ログの種類

SYNESIS が出力するログの種類およびローテーションの設定は、下表の通りです。

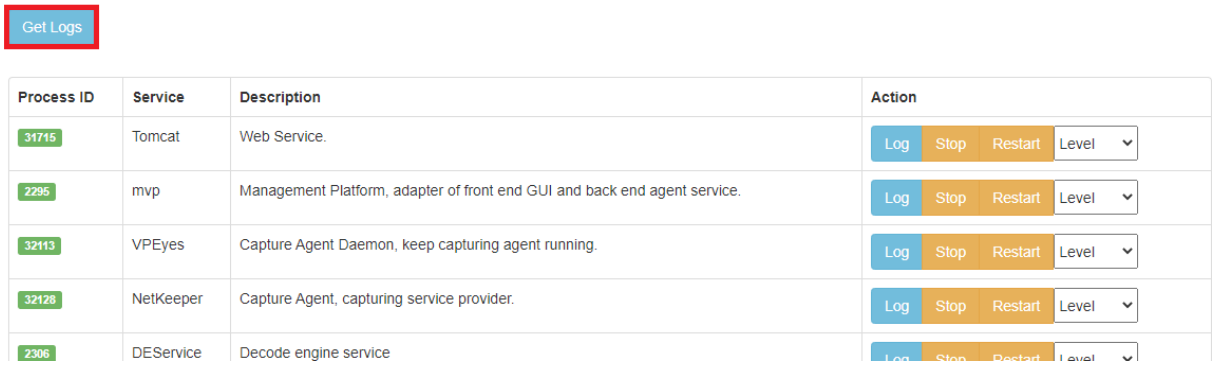
ディレクトリ名 ファイル名	[対象のプロセス] ログの内容	ローテーション設定
/opt/pvc/mngment-console		
pvc-mngment.log	[Management Console] Management Console ページの操作	
/var/log/		
syslog	OS 全般	日次でローテート 30 世代保持
ufw.log	[ufw] Firewall	週次でローテート 4 世代保持
/var/log/postgresql		
postgresql.log postgresql-12-main.log	[PostgreSQL] 管理 DB アクセス時のエラー・警告ログ	週次でローテート 10 世代保持
/var/log/pvc/tomcat/		
polyvirtual_portal.log	[tomcat9] SYNESIS GUI 用の Web サーバ	10MB 毎にローテート 50 世代保持
/var/log/pvc/pktagent/		
NetKeeper.log	[NetKeeper] キャプチャ・解析	5MB 毎にローテート 5 世代保持
AppWars.log	[NetKeeper] 解析	同上
FeedService.log	[FeedService] パケットストアからの直接読み出し機能	同上
FlowKeeper.log	[NetKeeper] MFA	同上
FlowZoom.log	同上	同上
DEService.log	[DEService] Web デコード	同上
VPEyes.log	[VPEyes] NetKeeper プロセスの死活監視	同上
PacketFeed.log	[SYNESIS FS] ファイルシステムを利用した パケットストアからの直接読み出し機能	同上

CommandAgent.log	[CommandAgent] 各種スクリプトの実行	同上
/var/log/pvc/mvp/		
pvc_mvp_log_file	[mvp] Tomcat と NetKeeper の通信仲介	5MB 毎にローテート 15 世代保持
/var/log/pvc/notifier/		
Notifier.log	[Notifier] SYNESIS GUI 上で設定できる 通知機能の実行	10MB 毎にローテートし 50 世代保持
/var/log/pvc/nginx/		
access_doc.log	[nginx] SSL/TLS 化のための リバースプロキシサーバ	日次でローテート 14 世代保持
access_mgmt.log	同上	同上
access_synesis.log	同上	同上
error.log	同上	同上
/var/log/pvc/synesisfs/		
SynesisFS.log	[SYNESIS FS] ファイルシステムを利用した パケットストアからの直接読み出し機能	5MB 毎にローテート 5 世代保持
/var/log/toyo/		
PacketReplayer.log	[PacketReplayer] CLI 版パケットリプレイヤー	日次でローテート 14 世代保持
PacketReplayerSync.log	[PacketReplayerSync] タイミング同期版パケットリプレイヤー	同上
TcpRedirect.log	[TcpRedirect] CLI でのパケット編集	同上
adapterProfile.log	[adapterProfile] リンク速度・モードの切り替え	同上
backupRestore.log	[BackupRestore] GUI 上での設定バックアップ・リストア	同上

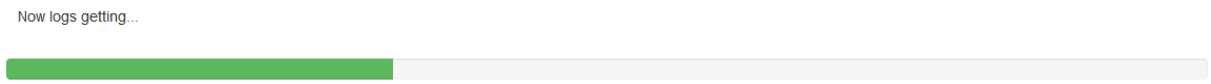
11.2. ログの取得方法

SYNESIS のログ取得手順について説明します。

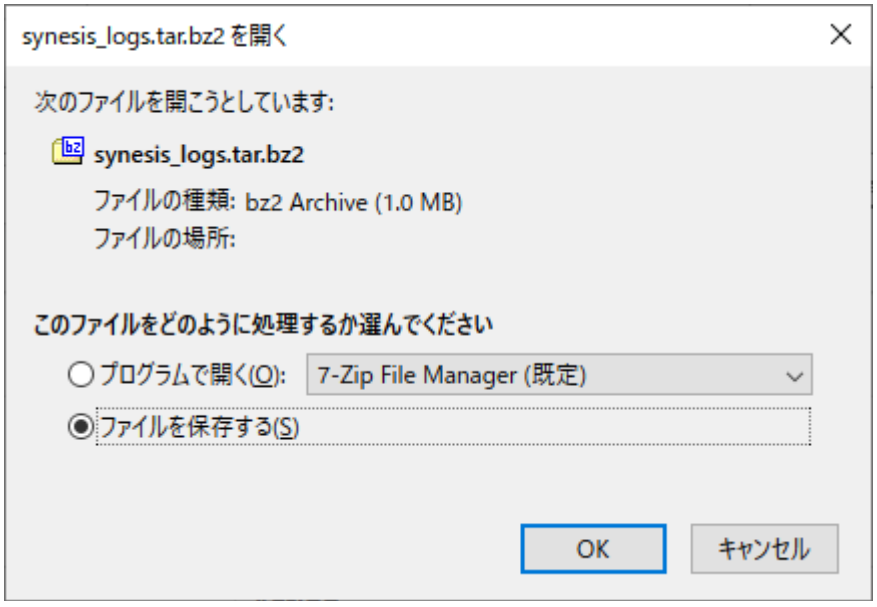
1) 「3.3.2. Management Console」の「3.3.2.1 ログイン」を参考に、Management Console にログインします。
2) 以下の Management Console が表示されます。**[Get Logs]**をクリックします。



3) ログの収集には 1~2 分を要します。以下のようにプログレスバーで進捗状況が表示されます。



4) 以下のダイアログが表示されますので、ログを保存してください。



synesis_logs.tar.gz2 には「11.1 ログの種類」で示されるファイルの他に、以下の情報も含まれます。

ファイル名	ログの内容	手動で取得する際のコマンド
etc/pvc/*	SYNESIS 構成情報	`$ sudo cp -r /etc/pvc .`
etc/nginx/*	nginx 構成情報	`$ sudo cp -r /etc/nginx .`
etc/netplan/*	管理ネットワーク構成情報	`$ sudo cp -r /etc/netplan .`
etc/resolv.conf	DNS サーバ情報	`$ sudo cp /etc/resolf.conf .`

hardware/cpuinfo.txt	CPU に関する情報	`$ sudo cat /proc/cpuinfo > filename`
hardware/lshw.txt	ハードウェアデバイスに関する情報	`$ sudo lshw > filename`
hardware/portinfo.txt	キャプチャモジュールのポートに関する情報	`$ sudo /usr/local/synesis/synesis_tools/GetPortInfo/main.sh > filename`
hardware/SSDCheck.log	SSD 診断情報	`$ sudo /usr/local/synesis/synesis_tools/SSDchecker/ssdchecker.sh` `$ cp /var/log/SSDCheck.log .`
hardware/arcconf.txt (Portable タイプのみ)	RAID コントローラ情報	`$ sudo /usr/local/sbin/arcconf GETCONFIG 1～N AL > filename`
hardware/arcconf_smartstats_*.xml (Portable タイプのみ)	RAID コントローラ情報	`$ sudo /usr/local/sbin/arcconf GETSMARTSTATS 1～N > filename`
hardware/sas2ircu.txt (Portable タイプのみ)	RAID コントローラ情報	`$ sudo /usr/local/sbin/sas2ircu LIST` `$ sudo /usr/local/sbin/sas2ircu 0～N DISPLAY noprompt > filename`
hardware/sas3ircu.txt (Portable タイプのみ)	RAID コントローラ情報	`$ sudo /usr/local/sbin/sas3ircu LIST` `$ sudo /usr/local/sbin/sas3ircu 0～N DISPLAY noprompt > filename`
hardware/msecli.txt (Portable タイプのみ)	RAID コントローラ情報	`$ sudo msecli -L > filename`
hardware/omreport_system_esmlog.txt (Distributed タイプのみ)	Dell ハードウェアログ	`$ sudo /opt/dell/srvadmin/bin/omreport system esmlog > filename`
hardware/omreport_system_alertlog.txt (Distributed タイプのみ)	Dell アラートログ	`$ sudo /opt/dell/srvadmin/bin/omreport system alertlog > filename`
hardware/omreport_system_cmdlog.txt (Distributed タイプのみ)	Dell コマンドログ	`$ sudo /opt/dell/srvadmin/bin/omreport system cmdlog > filename`
hardware/lsi*.log (Distributed タイプのみ)	Dell ストレージコントローラログ	`$ sudo /opt/dell/srvadmin/bin/omconfig storage controller action=exportlog controller=0～N` `$ sudo cp /var/log/lsi* .`
opt/napatech3/info/supportinfo-*.tar.gz	キャプチャモジュール情報	`$ sudo /opt/napatech3/bin/supportinfo`

opt/napatech3/config/*	キャプチャモジュール構成情報	`$ sudo cp -r /opt/napatech3/config .`
system/ps.txt	プロセス情報	`$ ps auxww -L > filename`
system/pstree.txt	プロセス情報	`$ pstree -p > filename`
system/ls-core.txt	コアファイル情報	`$ ls -l /data/cores > filename`
system/df.txt	ファイルシステム情報	`$ df -h > filename`
system/du.txt	1GB 以上のファイル一覧	`$ du / -h | grep [0-9][GT] > filename`
system/fdisk.txt	ディスクパーティション情報	`$ fdisk -l > filename`
usr/local/synesis/synesis_tools/*	各種ツール用構成情報	`$ sudo cp -r /usr/local/synesis/synesis_tools .`
usr/local/synesis/log/*	パッケージインストールログ	`$ sudo cp -r /usr/local/synesis/log .`

12. 障害・異常発生時の対応手順

SYNESISで障害と思われる事象が発生した場合は、弊社のSYNESISサポートグループまでお問い合わせ願います。お問い合わせの際には、以下の情報をご連絡ください。

- **発生した事象のまとめ**
- **簡易動作確認の実施と結果の確認**
- SYNESISのログ

12.1. 発生した事象のまとめ

障害と思われる事象に関する情報(SNMP Trap, Syslog, LEDの内容、等)の収集をお願いします。

- 通常青色で点灯のHW LEDがオレンジ色で点滅している
- iDRACからSNMP Trapを受信した
- SYNESISを操作できない

12.2. 簡易動作確認の実施と結果の確認

障害と思われる事象が発生した場合には、「**10. 簡易動作確認手順**」に従って簡易動作確認を実施してください。

確認の結果、問題があった場合は、問題があった箇所の画面キャプチャを取得してください。

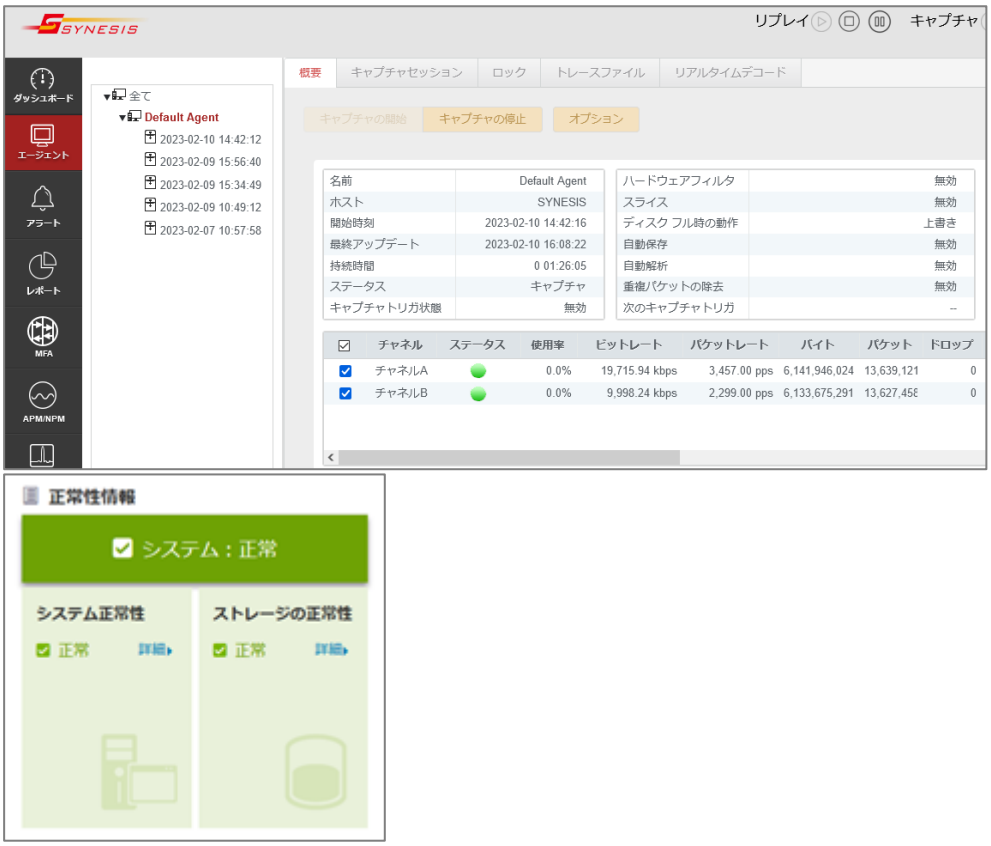
※画面キャプチャが取得できない場合、下記の情報をご提供ください。

□ SYNESIS のポートごとのステータスが「緑」になっているか。

□ SYNESIS の各統計値がキャプチャ中に更新されているか。

□ SYNESIS の「ドロップ」欄のカウントが 0 であるか。

□ iDRAC ポートの「正常性情報」欄が、全て緑のチェックとなっているか。



12.3. ログの取得

「**11. ログの種類と取得**」に従い、ログの取得をお願いします。

12.4. お問い合わせ

お問い合わせ内容と共に「12.1～12.3 にて確認・取得した情報」を下記弊社サポート宛てへお送りください。

[問い合わせ先]

株式会社東陽テクニカ

技術部 SYNESIS サポートグループ

TEL：03-3279-0771(代表)　03-3245-1107(直通)

FAX：03-3246-0645

E-Mail　：synesis-support@toyo.co.jp

受付時間：月曜～金曜 9:30~17:30 (土日、祝日、年末年始および弊社指定休日を除く)

更新履歴

Revision	Date	Content
Rev.A	2017/12/22	初版
Rev.B	2018/11/05	V4.0
Rev.C	2020/2/26	V5.0(html 化)
Rev.D	2020/8/6	V5.5
Rev.E	2021/1/22	V6.0
Rev.F	2021/3/5	V6.0.4 iDRAC8 対象モデルが EoS のため記載を削除
Rev. 6.0.6.1	2021/4/23	レイアウト・相互参照の修正
Rev. 6.5.1.1	2021/9/30	V6.5
Rev. 6.5.2.1	2021/10/26	4.1.3 管理ポート(GUI)の補足を削除
Rev. 7.0.1.1	2021/12/28	V7.0
Rev. 7.0.3.1	2022/2/28	V7.0.3 ボンディングインタフェース設定例の追加
Rev. 7.5.1.1	2022/9/30	2.5 キャプチャカードの再起動コマンドを変更 4.2.1.1 GUI での Firewall 設定確認を追加 4.2.3 IPv6 アドレス使用時の設定方法を追加 5.1.1.2 OS アカウント作成時のデスクトップアイコン設定を追加 5.1.2.1 OS アカウント変更時の Firefox 設定を追加 7.1.4 故障検知を無効化するパラメータ名を修正
Rev. 8.0.1.1	2023/3/31	4.2.6 CIFS を使用したストレージ共有の章追加 4.3.1.2 アクセス制限の設定手順を追加 6.4 Management Console：SYNESIS の異常監視の章追加 6.5.3 Trap 通知の旧仕様と新仕様の説明を追加 11.2 取得可能なログの一覧表を追加 用語の変更に伴う修正